

Toward Higher Flexibility of Federated Business Processes with Cloud-based Biometric Authentication Services

Christian Senk, Florian Obergrusberger, and Dieter Bartmann

Business Information Systems Management, University of Regensburg

Article Info

Article history:

Received May 18, 2014

Revised

Accepted

Keyword:

Authentication

Biometrics

Business Process Flexibility

Cloud Computing

Security as a Service

Trust Management

ABSTRACT

Access control to Web-based services in organization-spanning business processes requires the establishment of a trust relationship between the requesting user and the service provider. In identity federations the attestation of a strong user authentication by the users' identity provider might reduce trust management requirements at the organizational level, thus potentially increasing the flexibility of this relationship. With this said however, the availability of strong authentication controls at the identity provider's site, that is, for two-factor authentication, cannot be generally assumed. Thus, a service provider's attempt to enforce the use of such systems in turn reduces structural flexibility. This paper proposes a cloud-based biometric authentication system, provided by an external authentication service provider, which enhances existing identity management infrastructures flexibly on an on-demand basis by sustaining authentication through a second factor. Here, a generic architecture for cloud-based biometric systems and a prototype implementation based on keystroke dynamics is provided. The biometric system features low dependence on dedicated sensory hardware and thus leverages the structural flexibility of a security infrastructure. Additionally, it provides for end-to-end integrity mechanisms between the authentication service provider and the identity federation's business service provider to further improve access control.

Copyright © 2014 Institute of Advanced Engineering and Science.

All rights reserved.

Corresponding Author:

Christian Senk

University of Regensburg

Universitaetsstr. 31, 93053 Regensburg, Germany

christian.senk@ur.de

1. INTRODUCTION

The execution of business processes requires the underlying infrastructure to restrict access to respective *Information Technology* (IT) resources to authorized subjects. Within an organization's own domain this can be effectively provided for with centralized *Identity and Access Management* (IAM) systems [1, 2]. With this said, ensuring secure access to IT resources (e.g. Web-based services or documents) in inter-organizational applications is challenging [3, 4]. Especially in scenarios with substantial structural flexibility requirements such centralized approaches are less applicable because of the high costs for the creation and maintenance of redundant user accounts involved [2, 4]. This disadvantage can be circumvented by distributing the *Identity Management* (IdM) to the respective user's home organization [5, 2]. In this context, technologies for *Federated Identity Management* (FIM) gain increasing importance for the implementation of security infrastructures supporting the execution of flexible inter-organizational business processes [2, 6]. However, related approaches restrict control options for resource owners since key IdM functions such as authentication are controlled externally [2, 6, 4]. Both rising demands for (inter-organizational) flexibility [7, 8, 9] and the increasing importance of *Information Systems'* (IS) compliance with legal and regulatory requirements [10, 11, 12] indicate deficiencies in the assumed trust model, especially for *highly flexible Business Processes* (hBP) which are currently the focus of the research association "forFLEX"¹ [4, 13]. Here, provable strong user authentication provides an additional level of control and thus potentially reduces requirements for the trust management at the organizational level [14, 4, 15]. Consequently, knowledge-based authentication will significantly lose relevance while both token-based and biometric methods will get much more important in IT applications in the next

¹Focus: Service-oriented IT-Systems for highly flexible Business Processes, see <http://www.forflex.de/index.php/en>

few years [16]. In this regard, biometric authentication is advantageous because of two reasons. Firstly, the application of token-based systems is involved with high efforts for the personalization and distribution of respective dedicated hardware devices, which directly restricts flexibility compared to certain biometrics [17, 18, 4]. According to a survey conducted in 2012 by GEMALTO among 500 IT decision makers in Europe and the United States, costs are the primary obstacle for organizations' investments in strong (or strengthening) authentication systems [19]. Secondly, only biometrics can provide for a native personal reference to the person to be authenticated [20, 17, 18, 4]. Tokens (as well as passwords) can thus easily be transferred to arbitrary individuals and are not inherently bound to their legitimate owner [17, 18, 4]. Despite these benefits there is no high diffusion of respective systems in networked applications, yet [21, 22]. The *Cloud Computing* model promises higher organizational and technical flexibility and therefore decreases entry barriers for various IT systems [23, 24, 25]. Since it also potentially leverages the diffusion of strong authentication systems, it should be considered for the implementation of a possible biometric solution. To the authors' best knowledge such an artifact does not yet exist. The derived research question is concerned with how to design a cloud-based biometric authentication system for the enhancement of existing infrastructures, which supports the execution of business processes in federated environments (referred to as *Federated Business Processes*). The design should not substantially constrict structural flexibility, or in reverse, increase the flexibility of such IS considering existing security level agreements. In light of the points mentioned above, the main contribution of this paper is the development of such a system following the design science approach. Because of very advantageous characteristics such as its low relative dependence on dedicated hardware and its positive performance from a data protection point of view, we exemplarily apply a method based on keystroke dynamics [26, 18, 4, 27]. The remainder of this paper is structured as follows: The next section provides the theoretical background for this paper. In Section 3. system requirements are specified. The subject of Section 4. is the design and prototype implementation of the system, which will then be technically evaluated in Section 5. and comprehensively discussed in Section 6.. In Section 7. related work is laid out. Finally, Section 8. summarizes the results of this paper and discusses directions for future research.

2. THEORETICAL BACKGROUND

This section lays out the theoretical fundamentals for this paper's conceptual work including distributed IdM, related trust issues, biometric authentication as one possible way to leverage trust, and *Cloud Computing* as a promising delivery model for respective services.

2.1. Federated Identity Management

Enterprise IdM encompasses all of the functions necessary to identify users of IS and to assign them the exact privileges they require to achieve their business tasks considering effective access control policies [28, 20, 2, 29]. This includes controls for authentication, authorization, accounting, and auditing [2, 29]. In this context, user identity is defined as a user identifier in combination with additional descriptive user attributes [5, 30]. Increasing structural and behavioral flexibility demands of modern business processes pose a challenge for IS design and implementation [13]. Key requirements for an inter-organizational IdM to support hBP include (1) the structural flexibility of the required infrastructure and (2) a sufficiently high degree of control over subject attributes at the point of access [2, 4]. Here, the correctness and quality of information regarding user identities is a prerequisite for an informed access control decision, and on the other hand is also necessary to assign unambiguous requests in retrospect to a natural person and to provide for auditability [28, 2]. Intra-organizationally speaking, IdM is usually employed applying the IAM model [2]. IAM focuses on the cross-application centralization of identity data. For this, a centralized identity repository is fed by leading systems (e.g. *Human Resource Management* systems) with relevant user-related information to selectively provide target systems (e.g. internal business services) [2]. This induces cost and quality benefits and also enables enterprise *Single Sign-On* (SSO) [2]. Indeed, IAM systems leverage direct control of user-related data within a security domain but lead to inefficiencies for user account management in inter-organizational settings and thus do not provide structural flexibility [2, 4]. This problem is addressed by FIM, which is defined as a model for distributed IdM in a formation of administrative independent entities [2]. This formation is referred to as *Identity Federation*. Both the authentication process and identity data is autonomously managed by a user's home organization (*Identity Provider*, IdP) and asserted to *Service Providers* (SP) if requested [2]. SPs own and provide Web-based business services for users within an *Identity Federation* and are thus responsible for appropriate access control. Since a user is authenticated by the corresponding IdP, an SP does not necessarily know the users which request access to specific resources [14, 2]. Because the corresponding access control decisions rely on its contents, the SP has to trust the IdPs' respective statements' validity [5, 14, 2]. *Trust Management* is thus crucial for FIM and usually based on explicit *Service Level Agreements* (SLA) between IdP and SP specifying minimum requirements to the security controls of federation members [5, 1, 31, 14]. The basic architecture of FIM, based on the reference architectures for

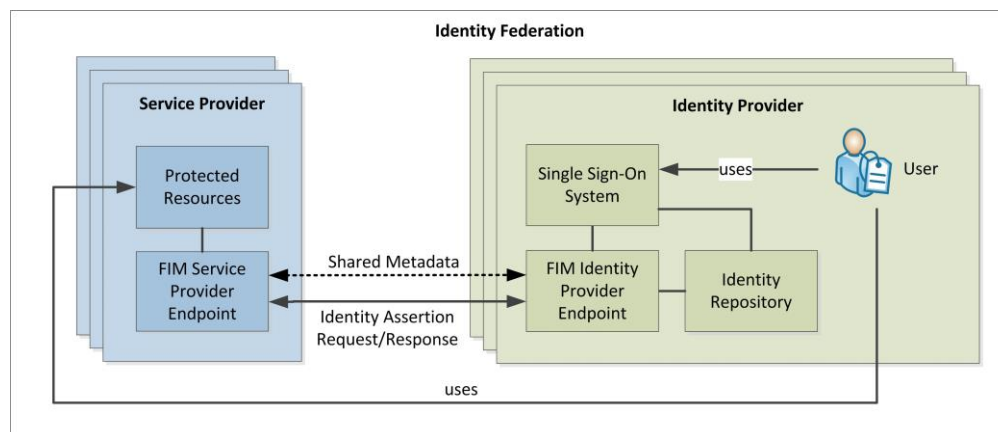


Figure 1. Basic Federated Identity Management Architecture.

FIM and IAM specified by [2], including the key roles IdP and SP, is depicted by Figure 1. The main benefit of FIM pertains to the efficiency and non-redundancy of user account management and thus a potentially higher structural flexibility in inter-organizational settings compared to the other IdM models [2, 4]. In principle, the FIM model is the right choice for the employment of an IdM for inter-organizational business processes in dynamic environments [4]. It enables an adequate level of identity data control and is more flexible than centralized approaches. Having said this, the structural flexibility of a business process spanning several organizations is still restricted by the required establishment of inter-organizational trust within the *Identity Federation* [1, 2]. The concept of FIM trust is laid out below.

2.2. Trust Model for Federated Identity Management

For informed and risk-adequate access control decisions the SP requires accordant certainty with regards to the accessor's identity which is provided by the corresponding IdP [1, 14]. This certainty is referred to as *Authentication Assurance* [32] or *Aggregated Direct Trust* [14]. GOMI proposes a comprehensive trust model for FIM [14]. According to this model, the *Aggregated Direct Trust*, in essence, consists of two elements: *Identity Trust* and *Attestation Trust* (Figure 2). *Identity Trust* is defined as the certainty that the identity of a user is identical with the identity he or she claims and is established by certain authentication procedures and the induced *Quality of Authentication* (QoA) [14]. *Attestation Trust* in contrast refers to certainty regarding the IdPs capability to "accurately create and assert information necessary [...] and to securely transmit the information" to the SP, that is using technologies such as SAML [14]. Hence, *Attestation Trust* covers the SP's organizational trust in the IdP and its IdM processes [32]. In certain environments organizations frequently join and leave an *Identity Federation* whilst measures to establish a certain level of *Attestation Trust* (e.g. by means of manual audits, SLAs, recommendation systems) restrict IS' desired structural flexibility. In these cases, the *Aggregated Direct Trust* can alternatively be leveraged by enforcing more sophisticated and strengthening authentication controls which increase *Identity Trust* and reduce access control risks [33, 14].

2.3. Enhancing Identity Trust with Biometrics

Users can generally be authenticated using knowledge-based, token-based or biometric methods [17]. Most systems implement basic password-based mechanisms (knowledge) [34]. However, because of humans' deficient cognitive ability to cope with sufficiently complex and thus secure passwords, and their inherent transferability, knowledge-based authentication mechanisms are considered to be insufficient for many applications [34, 35, 36, 37, 38, 39]. A possible way to increase the QoA is to replace or to supplement existing controls with token-based or biometric methods [14, 17]. The combination of different kinds of authentication methods is referred to as *Multi-Factor Authentication* (MFA) [17]. Biometric methods in particular are highly applicable for MFA since the respective authentication feature is inherently bound to its owner and cannot be easily transferred to other users [20, 17]. Authentication tokens do not natively provide for a binding to its legitimate owner, which induces vulnerabilities at the organizational level [20, 17, 4]. Furthermore, tokens must be personalized and physically distributed to the respective end users [17, 18]. This involves costs and time efforts, which reduces flexibility regarding the ease of employment

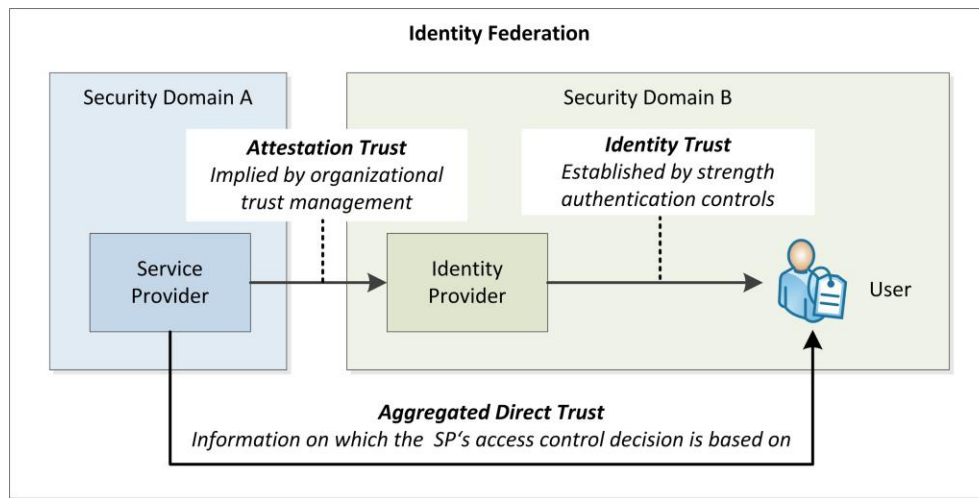


Figure 2. FIM Trust Model.

[17, 18, 4]. Biometrics in contrast only require a feature-specific (and not person-specific) sensor [17, 4]. A biometric authentication system may thus be employed independently from specific users and their possible sudden demand to be authenticated with a strong or second factor. Furthermore, certain biometric methods such as keystroke dynamics or voice recognition provide a low dependence on dedicated sensory hardware in standard working environments and can therefore be easily applied on short-notice [18, 4]. Biometric authentication is defined as the automated identification or verification of an individual, using behavioral or physiological features [17]. A prerequisite for biometric authentication is a prior enrollment phase in which the authentication system stores a biometric template generated from an individual's corresponding biometric feature [17]. During the authentication phase the user provides a biometric sample to be matched with the registered template [17]. Based on a predefined statistical threshold the system then decides whether or not a person belongs to the corresponding template [17]. A biometric system's performance is indicated by means of stochastic error rates, mainly *False Matching Rate* (FMR) and *False Non Matching Rate* (FNMR) [17]. The market for biometric authentication systems is still emerging [21, 22, 16]. Reasons for this include data protection, performance and quality issues whilst the cost of the dedicated sensory hardware required is also an issue [26, 22, 40].

2.4. Authentication as a Service

In FIM IdPs act as centralized autonomous sources for corresponding users' identity data and are responsible for proper authentication [2]. Since the fragmentation of IdM across IdPs and SPs induces technical and organizational problems [2], the IdP should be responsible for the entire authentication process and its coordination. Thus, an IdP must provide for the enforcement of adequate authentication controls according to an SP's requested QoA requirements. For instance, if an SP requests *Two-Factor Authentication* (2FA) the IdP must enhance its authentication system accordingly, that is, by employing a biometric authentication service. Respective (sub-) systems can either be operated internally by the IdP (on-premises) or outsourced to an external authentication service provider. Here, external security services which comply with *Cloud Computing* principles (referred to as *Security as a Service*, SE-CaaS) generally promise additional specific benefits compared to on-premises solutions or traditional security service outsourcing [27]. These benefits are predominantly induced by a relatively lower degree of resource binding due to external service provisioning and flexible license models [27]. It is with this in mind that, we focus our work on the application of the *Cloud Computing* model in order to reduce existing barriers to the application of multi-factor authentication systems [19]. Cloud-based authentication systems are referred to as *Authentication as a Service* (A3S). *Cloud Computing* comprises three sub-models, where *Software as a Service* (SaaS) specifically focuses on application software [41] including user authentication systems [27]. Key attributes of cloud services are listed below [23, 24, 25]:

- Application and underlying infrastructure are abstracted and offered through service interfaces;
- Standardized network/internet access by any device including thin client access for end users and standardized interfaces at the infrastructure level to provide for interoperability;

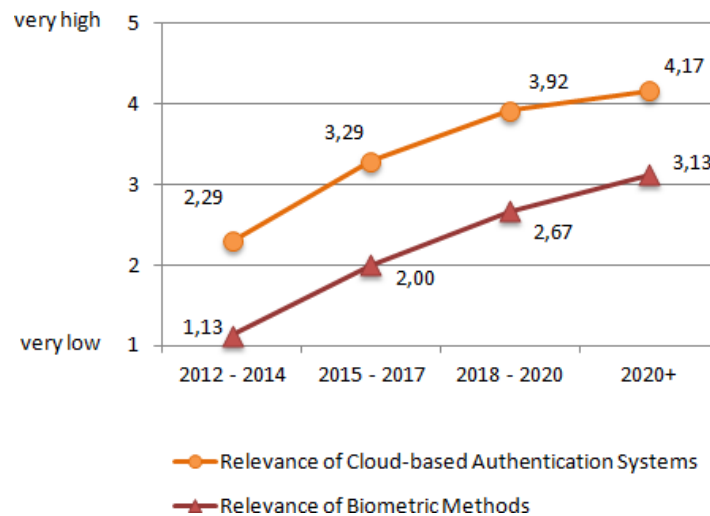


Figure 3. Development of the Relevance of Cloud-based Authentication Systems and Biometric Methods [16].

- Underlying infrastructure is scalable and flexible;
- Shared and natively multi-tenant resources which provide for data segregation and customizability;
- On-demand self-service provisioning and near real-time deployment;
- Flexible and fine grained pricing without up-front commitments.

Data collected in the course of a survey regarding the adoption of SECaaS solutions by enterprise clients indicates the relevance of A3S². Of 164 participating organizations, 12.8% plan to invest in cloud-based services for MFA within the next three years. This is strongly supported by the results of a recently conducted Delphi survey [16]. According to this 3-rounded expert study, the relevance of cloud-based systems for multi-factor authentication will substantially increase in the next few years [16]. Measured on a 5-point Likert scale where '1' indicates 'very low' and '5' represents 'very high', the expert panel³ estimated an increase of the significance of such systems from 2.29 (low) today to 4.17 (high) in the long run. Biometrics gain importance to a similar degree: from 1.13 (very low) today to 3.13 (medium) beyond 2020. Both developments are depicted by Figure 3. Whereas some token-based A3S implementations already exist, there is still a lack of consideration of biometric methods.

3. SYSTEM REQUIREMENTS

The specification of cloud-based authentication system requirements is based on a use case which was developed by the research association "forFLEX". First, basic architecture-related requirements for cloud-based authentication systems are specified. Second, the use case is described to derive application-specific requirements.

3.1. Cloud-specific Requirements

From general cloud service characteristics we specify the following design principles for A3S systems:

3.1.1. Abstracted and Standardized Service Interfaces

SaaS systems encapsulate a comprehensive and reusable functionality to coarse-grained services [42]. A3S services must provide for interfaces for end user registration, end user authentication, and service management. Service management includes functions for enterprise client account management, user management, service configuration, and monitoring. For strong end user authentication one authentication procedure or a combination of several

²Survey was conducted in cooperation with the German Federal Association for Information Technology, Telecommunications and New Media, Telecommunications and New Media (BITKOM e.V., see: <http://www.bitkom.de>); detailed data is not yet published

³consisting of 24 experts of the German-speaking area

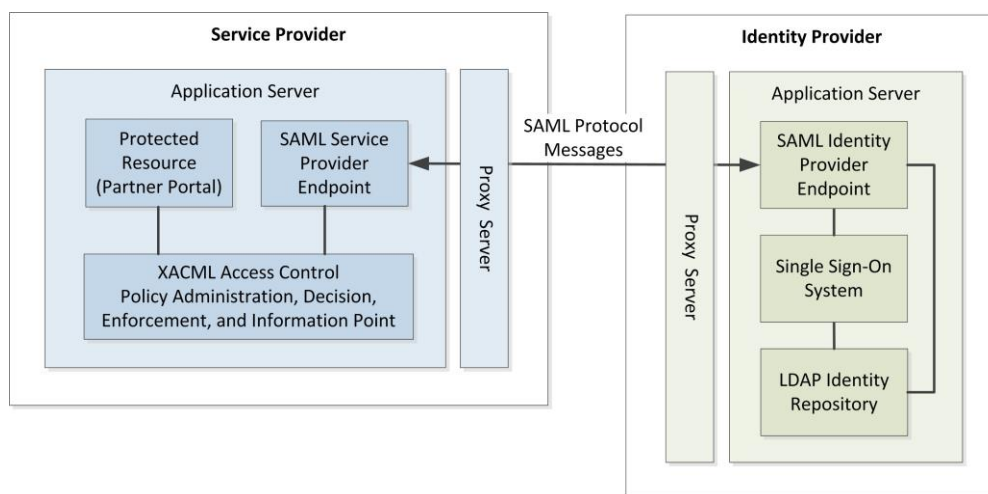


Figure 4. As-Is System Architecture.

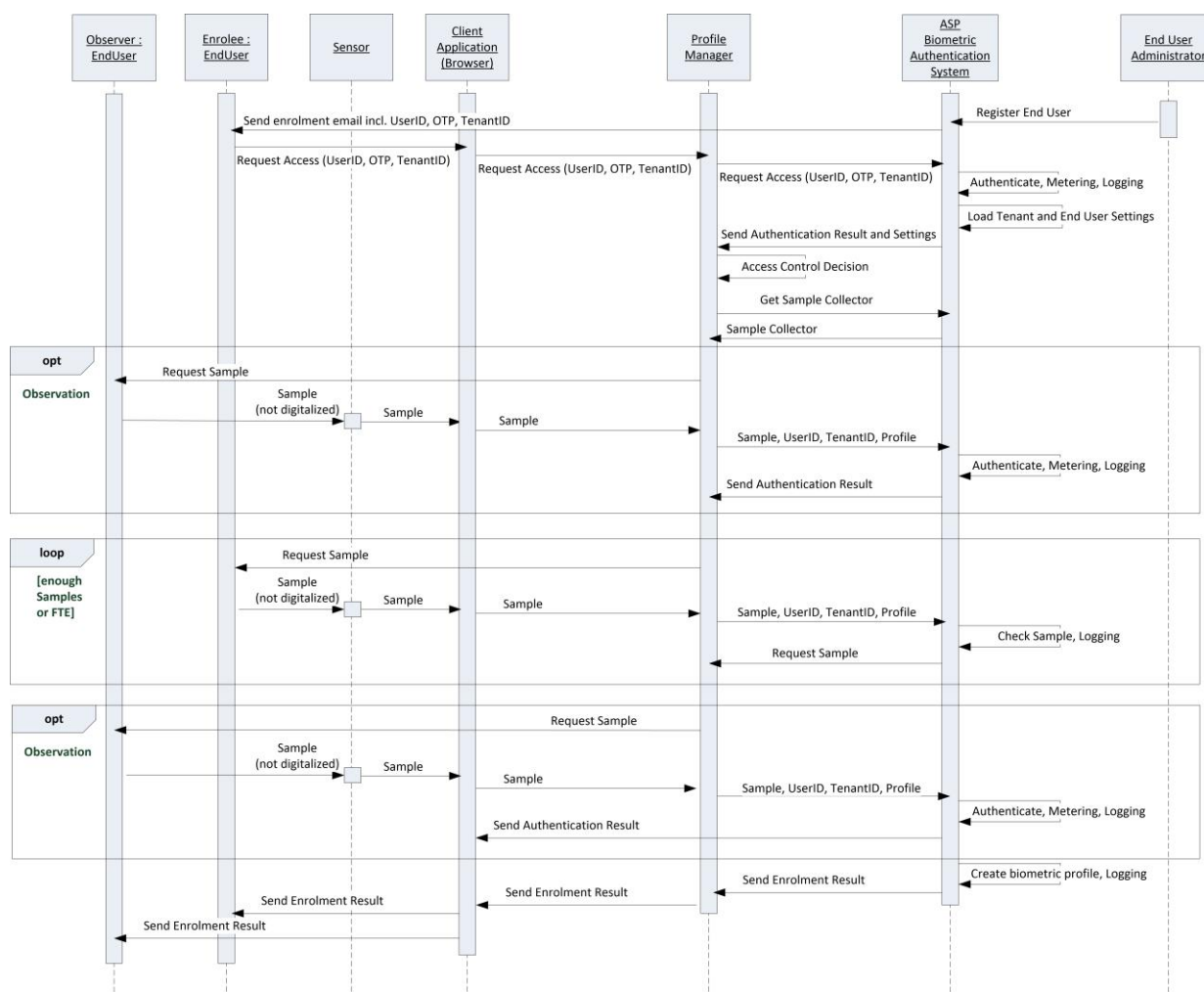


Figure 5. User Enrollment (Sequence Diagram).

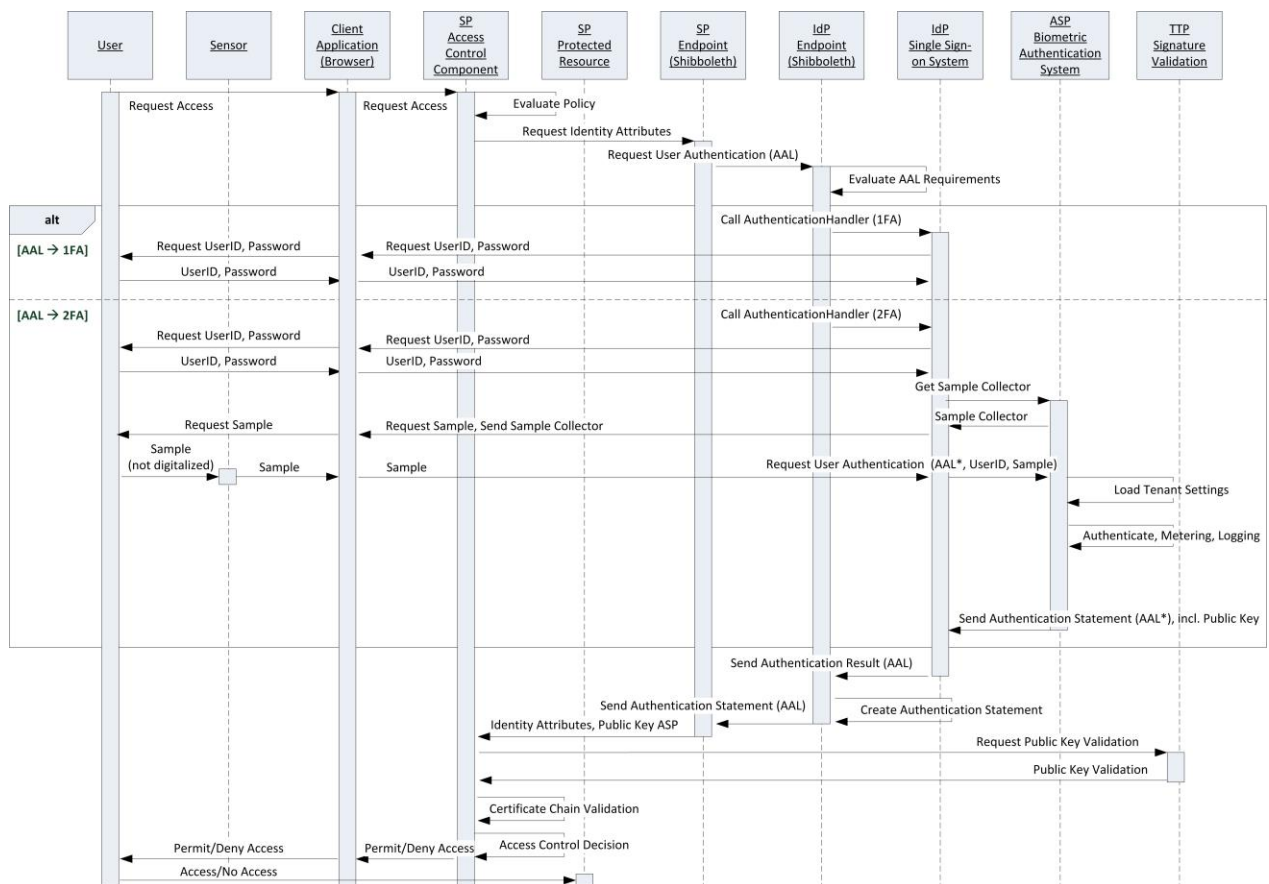


Figure 6. System Interaction (Sequence Diagram).

methods can be applied to achieve certain QoA levels [15]. Furthermore, the service might encapsulate either the entire authentication process or only parts of it. The corresponding authentication application and the underlying infrastructure have to be abstracted and offered through standardized service interfaces. Here, the SaaS model suggests a thin client service architecture [42]. Service interfaces should be accessible via Web browser without a necessity for the installation of dedicated hardware or software at the client side [42]. This not only induces specific requirements on the system's software architecture but also on underlying authentication methods. While knowledge-based procedures can simply be implemented on a pure software basis, token-based or biometric methods inherently require a corresponding hardware infrastructure. In light of this, comprehensive thin client architecture is only feasible when the hardware required is already sufficiently available in the context of use and is also in standardized form. Service interfaces must be standardized in order to leverage high interoperability and flexibility. This includes not only the thin client-based access to *Graphical User Interfaces* (GUI) but also interfaces for the integration of the service into the client's target infrastructure, that is, existing IdM systems [43, 44]. Relevant system interface technologies encompass the Web service specification, the *Lightweight Directory Access Protocol* (LDAP), and standardization in the realm of FIM including the *Security Assertion Markup Language* (SAML) and *WS-Federation* [45, 2, 46].

3.1.2. Flexible and Scalable Infrastructure with Native Multi-Tenancy

The authentication application has to be built on a scalable and flexibly composable infrastructure, which is shared among multiple enterprise customers (tenants) in a virtualized form. This enables economies of scale as well as the flexible and cost-efficient management of service capacities, e.g. to cope with a dynamic number of end clients [47, 48]. A system's ability to serve multiple tenants with a single system instance by providing for individual customizability is referred to as multi-tenancy [48]. Here, tenants are organizational units with specific application requirements renting such a system [48]. The concurrent access of different tenants' end users requires the shared application to isolate tenants appropriately [47, 49, 50]. For native multi-tenancy tenants are isolated at the SaaS application level [49]. GUO ET AL. describe three design patterns for data isolation with decreasing level of isolation [49]:

- *Totally Isolated*: Separate databases for each tenant;
- *Semi-shared*: Shared database for multiple tenants; separate tables and schemas for each tenant;
- *Totally Shared*: Shared database, tables and schemata for all tenants; records are mapped respectively.

The SaaS application must effectively control the access to tenant-specific resources. Here, in multi-tenant data models, either filter-based or permission-based patterns can be applied [51].

3.1.3. On-Demand Service Deployment and Service Use

The authentication service can be deployed, configured and used instantly (near real-time) without the need to manually set up a dedicated service instance at the provider's site. Here, the automated association of tenant-specific service resources is enabled by the application's native multi-tenancy. Since interfaces to the client infrastructure are standardized, no dedicated (proprietary) systems at the client's site should be required. The service is used on-demand on a self-service basis, that is, when a biometric authentication is required in addition to an internal basic authentication.

3.1.4. Flexible Pricing Model

In contrast with the more static outsourcing model *Application Service Providing*, SaaS is characterized by flexible pricing and licensing models with continuous payment and no required up-front commitments [24, 52, 43]. Here, usage-dependent and usage-independent assessment bases for pricing are differentiated [52]. Usage-dependent factors include the number of transactions, memory requirements, and the time of usage [52]. Usage-independent factors refer to, for example, a specific number of users and amount of master data [53, 52]. Hence, a suitable customer-oriented pricing model must be implemented.

3.2. Derivation of Specific Functional Requirements

The e-Car Ltd. is a fictional company which along with many others produces electronic cars. Consumers can flexibly customize new cars including multiple design options, that is, custom control elements. Here, the business process "Individual Parts Procurement" explicitly provides for the dynamic involvement of multiple manufacturers.

This is not entirely predictable and thus meets a key attribute of hBP. This imperfect ability to plan is based on the following circumstances: The contracting follows a tendering phase, which is conducted via an electronic marketplace system. Once a producer is awarded the contract, it will receive Web-based access to the detailed specifications of the affected vehicle model. For this purpose a partner portal (PP) has been implemented. Since the contained research and development knowledge of detailed specifications is critical to the success of e-Car Ltd., “very high” protection and corresponding access control requirements are induced. Therefore, a purely password-based authentication is considered insufficient. Technical specifications are processed within the company in the form of digital documents. In accordance with existing security policies, these documents may not be physically distributed (e.g. via e-Mail). Instead, they will be stored in a dedicated *Content Management System* allowing read-only access via Web browser. Web-based requests from external users should be protected through the enforcing of 2FA. To provide for efficient management of external user accounts the PP applies the FIM model and implements a SAML-enabled authentication interface. Here, e-Car Ltd. acts in the role of an SP, whereas external partners act as IdPs. When external users request access to resources with “very high” protection requirements, the corresponding IdP is forced to comply with this policy, authenticate users accordingly and to assert a successful 2FA via SAML. However, since it cannot be generally assumed that all IdPs operate 2FA systems, such access control policies exclude users from such IdPs and thus limit the structural flexibility of the affected business process. A possible solution artifact is a cloud-based authentication system (A3S) which provides interfaces to complement IdPs’ existing IdM infrastructures for 2FA in a cost-flexible way. Because of the positive attributes of biometrics regarding the realization of second factor authentication (*Factor-2-Authentication*, F2A, see Section 2.3.), an A3S system based on such a method is developed below.

4. SYSTEM DESIGN AND IMPLEMENTATION

The subject of this section is the development of a biometric A3S service, which meets the formerly identified requirements. Therefore, the assumed as-is-system is described first before the to-be-architecture for the federation is developed and the roles of ASP and *Trusted Third Party* (TTP) are introduced. A generic architecture for biometric A3S systems is specified afterward. The next subsection introduces keystroke dynamics and justifies its application in the present case. The prototype implementation of the biometric A3S service is then described in the last part of this section.

4.1. As-Is Infrastructure

In order to specify a starting position for further implementations, an FIM-based Web application was set up based on the use case described in Section 3.2.. The PP is represented by a Java EE Web application containing different sites with varying protection requirements. To enable a fine-grained and adaptive access control to these sections we defined access control policies using the de-facto standard *eXtensible Access Control Markup Language* (XACML, v2.0) [54, 30]. A FIM infrastructure was deployed using the field-tested open source system Shibboleth [55, 56]. It is based on the SAML standard (v2.0) and includes dedicated software systems for both IdP (v2.1.5) and SP (v2.3.1), which were installed on two separated servers. These two systems (FIM endpoints) were set up for an SAML-based communication using the SAML Web Browser SSO protocol and the HTTP-Redirect binding for IdP-initiated authentication [57]. A prerequisite for this communication is the previous exchange of metadata [55]. Following this, the two entities are able to exchange SAML statements via HTTP(s). The structure of the developed system is illustrated by Figure 4. Figure 6 depicts the interaction of relevant infrastructure components for basic *1-Factor Authentication* (1FA). When an external partner’s user requests access to a resource of the PP via Web browser, the access control component evaluates the corresponding XACML policy and requests the required identity-related attributes from the Shibboleth SP. This request is forwarded to the IdP’s FIM endpoint in the form of an SAML authentication request. This includes an `AuthenticationContext` attribute element. Its value specifies the required QoA. When the IdP’s Shibboleth system receives the SAML authentication request, the user is redirected to the internal IdM system’s centralized SSO portal. There, the user is authenticated via user name and password. Since no other automated authentication methods are available, the IdP cannot natively provide higher QoA if requested. Here, we assume the possibility that the IdP does not intend to invest in an on-premises solution for a token-based or biometric F2A, for example, due to economic reasons. If the authentication is successful the Shibboleth IdP sends an SAML authentication response including the specified `AuthenticationContext` element back to the requesting endpoint. Information regarding the attested user identity is forwarded to the access control component, which then decides whether or not the user is authorized to access the PP’s resources.

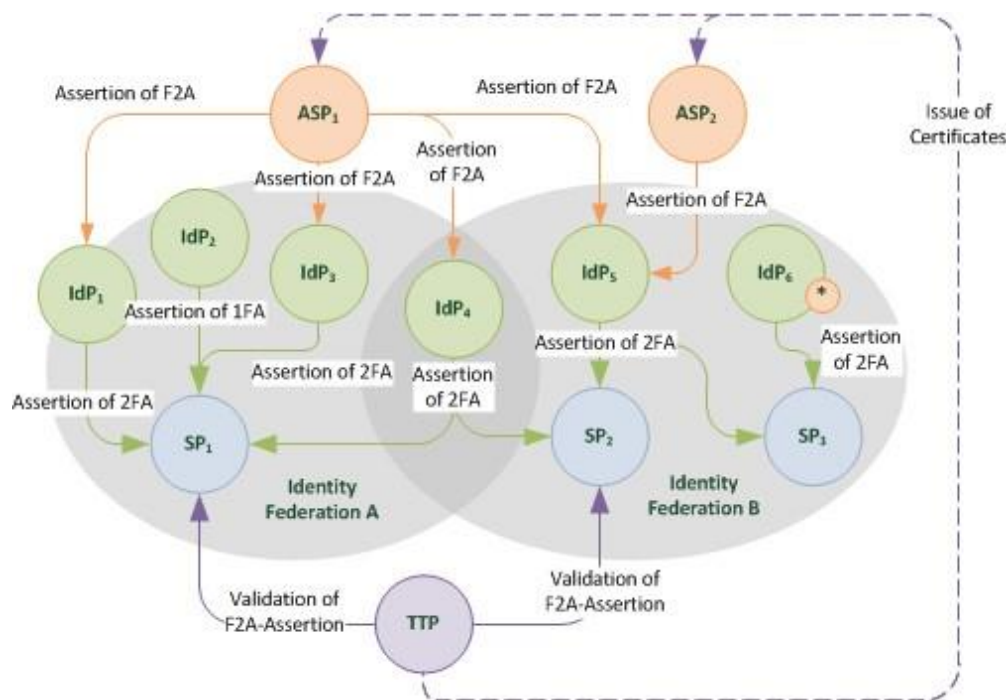


Figure 7. Extended FIM Infrastructure.

4.2. Extended FIM Infrastructure

Due to the restrictions of the basic FIM infrastructure setup, the IdP cannot provide for 2FA although this is explicitly requested by the SP via the SAML `AuthenticationContext` element. Based on the explanations of sections 2.3. and 2.4. this infrastructure will thus be extended by the two entities ASP and TTP. The resulting extended FIM ecosystem is depicted in Figure 7. ASPs operate and maintain A3S services for MFA complementing an IdP's 1FA with biometric F2A. Once deployed, the IdP's FIM endpoint is able to consume the A3S service automatically on-demand. Therefore, respective system interfaces must be integrated and appropriate decision logic implemented. If a user's 2FA is required, both *Factor-1-Authentication* (F1A) and F2A must be successful. Whereas F1A is natively conducted internally by the existing system, for F2A the user is logically forwarded to the external service where he or she is partially authenticated. A successful F2A is then attested by the ASP in standardized form to be processed by the IdP. If F1A is also successful the IdP attests the comprehensive 2FA to the requesting SP. However, a possible threat model from the SP's point of view is the IdP to forge F2A assertions. This can be restricted by the ASP signing respective attributes and thus allowing SPs to verify end-to-end integrity. Assuming a higher organizational trust between SP and ASP than between SP and IdP, this enhances the *Aggregated Direct Trust* between SP and user. For convenient validation of F2A assertions and the respective chain of certificates we employ a TTP.

4.3. Biometric Authentication as a Service Architecture

Figure 8 describes a generic architecture for cloud-based biometric authentication services based on related literature.

Customer Portal: This component provides information regarding the products offered, including functional range, price models and SLAs. The possibility to subscribe to such products (services) without human interaction fulfills the requirement of on-demand self-service provisioning [25]. Furthermore, the component covers business administrative tasks such as the update of contact or payment details, or the inspection of accumulated invoices.

Tenant Administration: This component allows for the (technical) customization of the service according to tenant-specific needs [41]. Moreover, the service capacity can be scaled including the number of end users to be authenticated biometrically whilst system events can also be monitored.

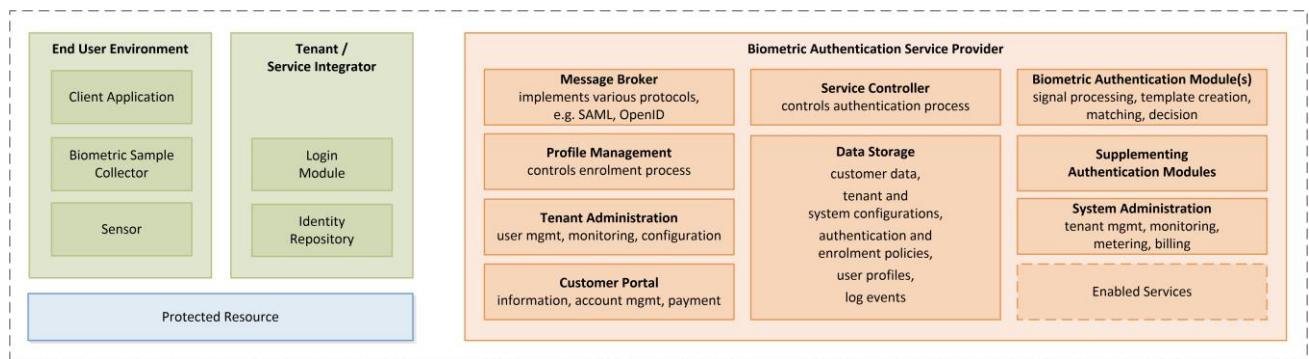


Figure 8. Generic Architecture for Biometric A3S Systems.

Profile Management: Prior to a biometric user authentication the system must be provided with a biometric template during the course of enrollment (Section 2.3.). Furthermore, certain biometric features involve aging and corresponding templates might require updates. For this purpose, the *Profile Management* component realizes an end user interface for the creation and maintenance of biometric profiles each including one biometric template and metadata.

Message Broker: Cloud services are accessed over the network using standardized protocols [41]. Based on specific protocols such as SAML or OpenID, an authentication service must enforce incoming authentication requests and respond accordingly [33]. This component receives such requests, translates respective demands for internal processing, and finally sends authentication responses using the original request protocol.

Biometric Authentication Module: This component implements biometric authentication logic including elements for signal processing, a comparison of the provided sample with the stored template, and authentication decision-making [58]. Tenant-specific parameters such as the biometric threshold are handed over by the *Service Controller*. The digitization of biometric data is conducted externally in the end users' environment.

Client Application: Access to server-sided resources is dealt with through a client-sided application. In case of SaaS, this is a Web browser [23, 24].

Biometric Sample Collector: This component utilizes a sensor for the digitalization of a biometric feature, transforms the sample into a target format and passes it over for further processing [59, 58].

Sensor: The sensor is a hardware component for the recording of specific biometric features and must be physically accessible to the person to be authenticated [34, 60].

Service Controller: User authentication must be enforced according to effective policies [33]. This component thus facilitates the management and evaluation of tenant-specific settings according to effective SLAs. Based on this data authentication modules are invoked with attendant configuration parameters.

System Administration: This component encapsulates internal functions such as the metering and billing, logging, as well as the modification of global system settings.

Supplementing Authentication Modules: Alternative authentication procedures, that is, for 2FA of privileged users, are encapsulated by this component.

Enabled Services: Further related functions which exceed the biometric authentication but are based on it are encapsulated by this component. Examples for such enabled services are the provisioning of user attributes or authorization statements.

Data Storage: Data such as user profiles, configurations as well as other customer- and security-related information are accessible for all system components over an independent data layer [33].

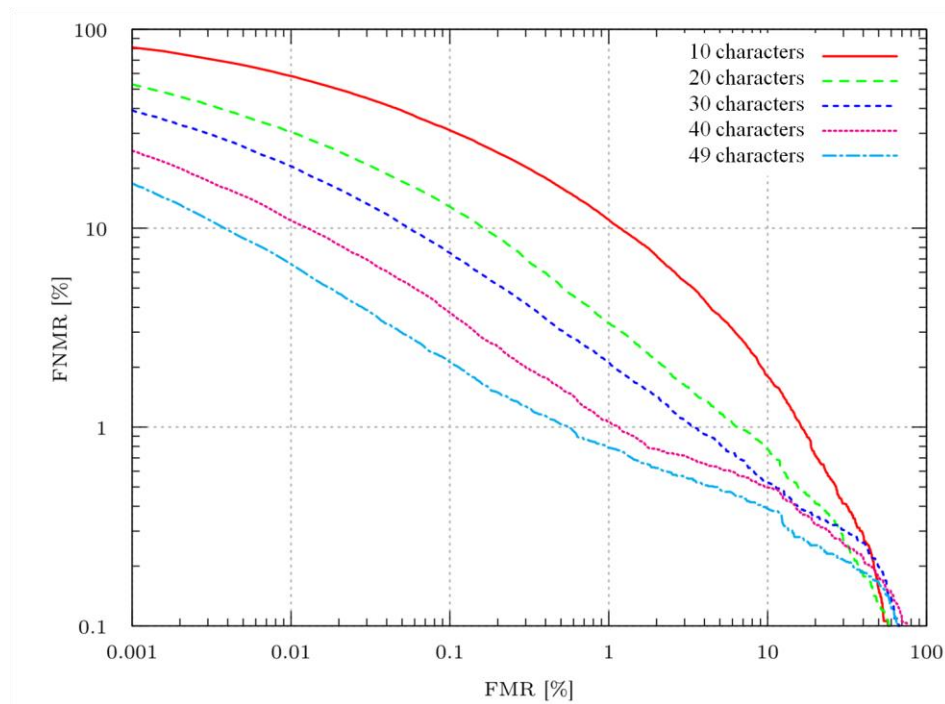


Figure 9. Performance of Keystroke Dynamics (Detection Error Trade-off Curve).

Login Module: The *Login Module* is responsible for receiving and identifying users intending to access specific protected resources. Therefore, it is the tenant-sided complement of the *Message Broker* and submits authentication requests, receives and evaluates authentication responses and triggers the access control component.

Identity Repository: This module encapsulates the target systems' identity management and is highly related to the *Login Module*.

Protected Resource: This can be any kind of Web-enabled service or application behind the *Login Module* implementing a constitutive access control.

4.4. Keystroke Dynamics

Below, the feasibility of the specified biometric service architecture is demonstrated applying keystroke dynamics for user verification. We applied keystroke dynamics as a suitable exemplary biometric method because of three major reasons: (1) It is easy and cheap to implement on a software basis; (2) keystroke dynamics does not depend on a particular piece of hardware; (3) it has advantageous attributes from a data protection point of view. Keystroke dynamics is an individual's strongly conditioned biometric feature and is determined by the sum of unique patterns regarding speed, rhythm, continuity and precision of typing as well as the finger pressure and placement in case of using a touch screen [61, 62, 63, 64, 65]. Hence, deeper attributes such as right- or left-handedness, symptomatic mistyping, correction behavior and dexterity can be utilized [59, 62]. On a computer keyboard, these characteristics are represented by a combination of key events (i.e. pressing and releasing of a key, hold and transition periods), which can be measured in the millisecond range [59, 62, 66]. The dependency of keystroke dynamics on a dedicated hardware infrastructure is very low compared to alternative methods such as iris recognition, where the availability of the required (dedicated) sensory infrastructure in a standardized way must be generally assumed [4]. Biometric systems based on keystroke dynamics are thus highly applicable for the implementation of Web-based systems such as cloud-based authentication services and are potentially cheaper to implement [67, 68, 18, 4, 16, 27]. Keystroke dynamics provide maturity levels qualified for broad practical use. Based on the FMR and FNMR, Figure 9 illustrates the performance of the keystroke dynamics method which was applied by the authors, tested by BEER⁴. At the reference

⁴Test details as stated in [62]: Number of users: 1,214; average number of typing samples per user: 30; number of enrollment samples: 10; number of attacker samples: 80

point FMR = 0.1%, the diagram indicates a FNMR smaller than 3% (2.12%) for keystroke dynamics based on an input text with 49 characters. It thus provides appropriate performance and security for practical use [69, 70]. Moreover, recent developments show significant increases regarding the performance of keystroke dynamics [62, 67, 71]. A biometric system's performance might depend on attributes specific to the quality of a certain sensor and its environment [17, 18]. Based on the consideration of two different keyboards, the work of GIOT ET AL. indicates that the accuracy of keystroke dynamics does not directly depend on certain keyboards used for enrollment and authentication [72]. We share this observation for different models of standard keyboards. However, we observed unexpected results using different keyboard layouts for the login on one biometric template. Thus, we enhanced our system with the option to use multiple biometric profiles (e.g. Profile A: US desktop layout, standard; Profile B: German laptop layout, standard). Since the authentication process can be performed with any keyboard of the same type or layout, a higher level of flexibility is provided compared to methods which require proprietary sensory hardware. Since both the adoption of SaaS and biometric technologies highly depend on perceived data protection and privacy risks, the compliance of a biometric A3S implementation with applying data protection regulations is essential in the organizational context [27]. In this regard, the better the data protection performance of a certain biometric feature and a respective authentication method, the easier is the legitimization of the comprehensive authentication system [26, 27]. The evaluation of a biometric characteristic regarding its data protection performance is based on its informational content, temporal variability, the risk of copying or theft, and the deliberate exertion of influence by the feature's owner. The informational content of keystroke dynamics does not breed any additional and potentially sensitive personal data that exceeds the purpose of authentication [26, 27]. In contrast, features such as face or voice might give implications about an individual's race or genetic diseases, which is rated critically from a data protection point of view [26, 27]. Moreover, a user constantly learns and thus refines his own typing [26]. This results in a high temporal variability, which is indeed positive in terms of data protection but -if not considered by system's design- might lead to its inability to assign the user's feature with the respective biometric template [26, 27]. While characteristics such as face, fingerprint or voice are quite exposed, keystroke dynamics is a strongly covert biometric feature [26, 27]. Last but not least, keystroke dynamics allows to deliberately influence the collection and the processing of the biometric data [26, 27]. This is not given for static features such as fingerprints or iris patterns [26, 27]. As depicted by Table ??, keystroke dynamics performs best among the selected biometric characteristics.

With these relative benefits in mind, we base the prototype developed and implemented in the present work on such a method. In this regard, we applied a fixed text procedure (in fact the one depicted in Figure 9) that uses a constant text string for both to train a biometric profile and to verify a user subsequently. Such methods collect decision-relevant biometric information more efficiently than alternative approaches allowing variable and arbitrary text inputs [59, 62, 67]. Those require a proportionally higher amount of text to reach a similar recognition performance which again reduces user experience [59, 62, 67, 71]. Furthermore, fixed text methods are preferable over free text procedures from a data protection point of view [26, 27]. Such procedures consequently "restrict the collection, processing, and storage of biometric data to the required input text and avoid the creation of sensitive personal data" [27]. This ensures transparency to the user, which is always knowingly and willingly involved in the authentication process and the risk of covert surveillance or profiling is prevented [26, 27]. Furthermore, since a biometric template is bound to one specific input text, this can be devaluated and replaced by a new reference text in the case of compromise [26, 27]. Thus, stolen samples or templates then cannot be misused for further authentication transactions [26, 27].

4.5. Prototype Implementation

A brief overview of the prototype implementation is provided in this sub-section. This includes the biometric A3S service provided by the ASP, the integration of its system interfaces to an IdP's IdM system, and extensions for attribute validation at an SP's site. All components are implemented in the form of Java EE Web applications. The corresponding system behavior is illustrated by Figure 6 assuming that a user is already enrolled at the biometric system. Figure 5 depicts the enrollment process, which was enhanced according to OBERGRUSBERGER ET AL. in order to ensure the quality and authenticity of the biometric profile created in open Web-based environments [73].

Customer Portal: This application offers basic services for enterprise customers (e.g. represented by administrators in an organization's IdM department) similar to a online shop for authentication services. Here, customers' *Business Administrators* create and manage individual accounts and set up virtual authentication services. Furthermore, the application covers billing functionality.

Tenant Administration: *Service Administrators* can customize single authentication service instances according to individual needs. This includes parameters such as the input text used for authentication, the number of required

samples for user enrollment, and the threshold of the biometric system. Furthermore, a service user management is implemented. For the creation of user accounts, an LDAP-based connection to the customer organization's identity repository can be established to select certain users and to import user identities and e-Mail addresses. Following this, selected users get one-time access to the enrollment application via e-Mail. Administrators can increase the security of the enrollment process by enforcing a four-eyes-principle. Here, a previously enrolled trustworthy user (*Observer*) is selected to observe another user's enrollment.

Profile Management: To ensure that service use can be controlled, only selected users get access to this application and the enrollment process. Hence, a predefined number of biometric samples is collected by the *Client Application* and a biometric profile is calculated before being associated with the corresponding user account. If the *Service Administrators* choose an *Observer*, this must be present during the entire process and authenticate twice via keystroke dynamics, once before the other user's enrollment and once after.

Message Broker: The *Message Broker* is a sub-component of a modified *Shibboleth IdP* instance. It accepts SAML-based authentication requests including user identifier, profile name, tenant identifier and typing sample. Biometric samples consisting of key events are coded as (encrypted) text string and received in the form of a dedicated SAML attribute value as illustrated in Listing 1. This information is passed on to the *Service Controller*. The authentication result is returned to the *Message Broker*, which then builds and submits the authentication response to the requesting party. The authentication response includes the biometric authentication status (successful or not) with timestamp, information regarding the applied method, the signature for the biometric authentication status, and the ASP's corresponding public key.

Listing 1. Authentication Request with Biometric Sample

```
<?xml version="1.0" encoding="UTF-8"?>
<samlp:AuthnRequest
  xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
  AssertionConsumerServiceURL=https://sp/Shibboleth.sso/SAML2/POST
  Destination=https://idp/idp/profile/SAML2/Redirect/SSO
  ForceAuthn="1" ID="_5c2e5253ef57eff6db467bd4456211fd"
  IssueInstant="2012-03-16T08:17:33Z"
  ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Version="2.0">
  <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
    https://pcrw00032.uni-r.de
  </saml:Issuer>
  <samlp:NameIDPolicy AllowCreate="1"/>
  <samlp:RequestedAuthnContext>
    <saml:AuthnContextClassRef xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
      urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified
    </saml:AuthnContextClassRef>
  </samlp:RequestedAuthnContext>
  <samlp:Extensions>
    <method>keystroke_fixedtext</method>
    <uid>sec18340</uid>
    <profile>standard</profile>
    <tenantid>uni-r</tenantid>
    <sample>!01!fb5xL0dvt/PUaqbySNXp00hP2x1RjUUX+ BEQ0KtSmIbU76cJaItHIQHahZO5CuDt8aKEVKHdsy6 GFnFyMxd3A/
      oNiyvU1Te4MFQMP7t90FVvahkc7GFu/ QwI8H6J1LPK53eyUwbE+fznflHNlxDvo4N1z00QrT
      MA2qVqRWvItt2EaM9RaZzi7as2R2On8RkSziSQxLiD <!--cropped for reasons of visualisation-->
    </sample>
  </samlp:Extensions>
</samlp:AuthnRequest>
```

Biometric Authentication Module: The central element is an existing biometric system for keystroke dynamics implementing a fixed-text procedure. This system is based on the work of BAKDI [59] and provides the methods necessary for signal processing, template creation, matching, and decisions. It was provided to the authors for research purposes⁵. The biometric authentication module implements a mechanism for adaption in order to adjust the biometric template to constant refinements of an individual's typing. Furthermore, a control for replay or sensitivity attack prevention was implemented. The system's architecture explicitly provides for additional biometric authentication methods. However, we only applied one procedure in order to present a proof-of-concept implementation.

Biometric Sample Collector: Key events in the millisecond range are provided by the clients' operating systems. Since the *Client Application*, which is an arbitrary Web browser, cannot measure such data itself an additional component must be embedded in order to communicate with the sensor and corresponding drivers. For this purpose, the

⁵by Psylock GmbH, Germany

enrollment and authentication Web sites can implement a sample input field based on the client-sided Web technology *Flash*.

Sensor: The sensor is represented by a standard computer keyboard. A biometric profile is not bound to the keyboard used for enrollment. However, it is advantageous from a performance point of view to use similar keyboard layouts for enrollment and subsequent verification. Therefore, for different kinds of keyboards used a user might want to create different biometric profiles, e.g. for the parallel use of (1) a standard personal computer keyboard (US), (2) a notebook keyboard, and (3) mobile devices with touch screen input ⁶.

Service Controller: Based on the information provided by the *Message Broker*, the *Service Controller* loads tenant-specific security settings and calls the *Biometric Authentication Module* (keystroke dynamics) with respective parameters. Optionally, other authentication modules or enabled services can be invoked.

System Administration: This application allows administrators of the ASP to manage tenants, adjust system-wide settings and monitor system behavior.

Supplementing Authentication Modules: To enable 2FA for administrators we implemented a one-time password service sending credentials via SMS. Furthermore, this service can be used as an alternative procedure for handicapped users.

Data Storage: To provide for scalability all components share the database service of a well-known cloud infrastructure provider.

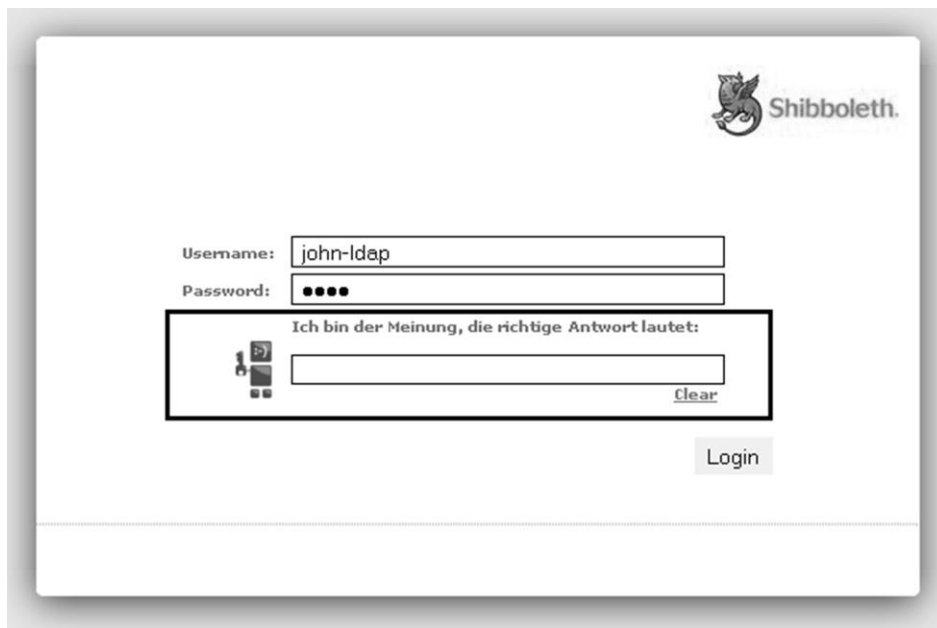
Login Module: The *Login Module* is responsible for receiving users, which intend to access a specific protected resource and initiate appropriate authentication procedures. It is represented by the *Shibboleth IdP* software containing a supplementing *LoginHandler* component. Dependent on the *AuthenticationContext* attribute value of an SP's authentication request, the *Shibboleth IdP* software delegates to either the native component for basic authentication or the 2FA *LoginHandler* enforcing both F1A and F2A. This component automatically embeds the *Biometric Sample Collector* into the SSO form displayed to the user to be authenticated (Figure 10) and loads respective settings dynamically. For this purpose, the ASP provides respective Web service methods. The SSO form inquires user id, password and typing sample. Once the form is submitted, user id and password are evaluated internally. Additionally, an SAML authentication request containing user id and sample is formed and sent to the ASP. As soon as both authentication results are available, the result of the comprehensive 2FA is returned.

Protected Resource: In the present case, the protected resource is represented by the *Shibboleth SP* and Web-based resources in the respective security domain. Authentication requirements are stated utilizing the *AuthenticationContext* element of the SAML authentication request message to be sent to the IdP. An access decision is made when appropriate user authentication has been attested by the IdP and other required information is available. In cases where that 2FA is required, the IdP's SAML authentication response includes the attribute for partial biometric authentication. Since the IdP processes this attribute to build a new assertion for the resulting comprehensive 2FA, it could easily be modified to fool the SP. To ensure the verifiability of the end-to-end integrity of the partial biometric authentication assertion, it is signed by an ASP using its private key. The signature can be checked with the ASP's public key, which was certified by a TTP. The TTP provides a Web service which SPs can call to get the root certificate and to validate the received public key of the ASP and thus the validity and authenticity of the biometric assertion attribute. This procedure implemented for the evaluation of key certificates was proposed by FOX [74].

5. EVALUATION OF THE PROTOTYPE IMPLEMENTATION

The main goal of this work was to implement an A3S system for enforcing and unforgeably attesting biometric F2A. As shown in the previous section, functional requirements were fully met covering the comprehensive customer process from service rent, administration, user enrollment, authentication, and billing. Beyond, we discuss the proposed system's compliance with the cloud principles defined (Section 3.1.): *Abstracted and Standardized Service Interfaces*: The implemented service provides an asserted biometric F2A which can be complemented to a 2FA in

⁶Keystroke dynamics on mobile devices with touch screen is not explicitly supported by the system implemented. However, there is ongoing research in that field. Respective methods or modules can be retrofitted.



The screenshot shows the Shibboleth login page. At the top right is the Shibboleth logo. Below it, there are input fields for 'Username:' (containing 'john-ldap') and 'Password:' (masked with dots). Below the password field is a section titled 'Ich bin der Meinung, die richtige Antwort lautet:' (I am of the opinion that the correct answer is:). This section contains a small icon of a person at a computer and a text input field. To the right of this input field is a 'Clear' link. At the bottom right of the form is a 'Login' button.

Figure 10. Single Sign-On Portal (Identity Provider).

the client's system. All end user interfaces are accessible via Web-browsers and thus realize the suggested thin-client architecture. Both the enrollment and authentication process require no dedicated hardware at the end users' side assuming office workspaces equipped with standard personal computer or notebook keyboards. However, the system is not feasible for use with mobile clients, yet. The applied authentication method (keystroke dynamics) is not optimized for respective input interfaces and alternative biometric methods have not been implemented. A tenant's target system must be able to build and send authentication requests to the A3S system and to process incoming authentication assertions. Since the employed FIM infrastructure was not able to distribute the authentication process over two or more domains, a generic non-authentication system-specific and non-provider-specific component was developed to be deployed in the tenant's IdM infrastructure for the secure exchange of authentication-related information between the IdP and the ASP. All system interfaces are either based on the SAML or SOAP Web service standard. Due to the deficient accessibility for mobile devices, the A3S prototype implementation does not fully comply with this requirement and is restricted to office applications. *Flexible and Scalable Infrastructure with Native Multi-Tenancy*: The proposed biometric A3S system was deployed in a cloud infrastructure fully scalable in terms of computing power and storage. The system provides for multi-tenancy at the application level using a shared database service. For enrollment and authentication the end users are mapped to the corresponding tenant. As proposed by HUANG ET AL. the *Implicit Filter Based Access Control Isolation* pattern was applied for data isolation, i.e. specific filters ensures that tenant-specific operations do not conflict with other tenants' data [51]. Hence, we consider the requirement to be fulfilled. *On-Demand Service Deployment and Service Use*: A prerequisite for service use is the initial creation of a tenant account by a customer's administrator. Following this, services with specific default functions and capacities can be logically deployed and associated with the tenant's account. The administration interface allows for the customization of each (logical) service, which must then be paired with the tenant's target system. At the tenant's side this includes the import of metadata, the upgrade of the IdM system's 2FA component, and optionally the interfacing of internal LDAP-based identity repositories with the authentication service's repository for higher ease of user management. Once the service is set up, selected end users can initially enroll to create their biometric profile and authenticate afterwards when F2A is required. Since the assumed target system at the tenants' side does not provide a standardized means for obtaining F2A from external domains, a time-consuming configuration is necessary and the possibilities of an on-demand deployment are substantially restricted. Hence, this problem can be mitigated by IdM software system providers natively providing for respective standardized interfaces. *Flexible Pricing Model*: The system's pricing is based on the number of end users managed by a specific tenant considering quantitative price discrimination; the higher the number of enrolled users the lower the average price for one user. Payments are due monthly. No long-term contracts or up-front commitments are provided for and indeed we deem them to be economically unnecessary from the ASP's point of view. Though the system is not in use in practice, we consider this requirement to be fulfilled.

6. DISCUSSION

This project involved the implementation of a cloud-based biometric authentication system to flexibly enhance authentication capabilities of IdPs in existing FIM infrastructures based on keystroke dynamics. It was deployed in a use case-specific SAML-enabled FIM infrastructure. This specific biometric method was used since it features very low dependence on dedicated sensory hardware and is thus highly qualified for Web and cloud applications. Moreover, the applied cloud model leverages high ease of use at the technical and the organizational level. Since the cloud service can cost-efficiently be applied on an on-demand basis, an SP's postulation of an increased authentication assurance level involving 2FA does not necessarily exclude certain IdPs, which are not capable of conducting such kinds of authentication. Here, a cloud service involves substantially lower entry barriers than alternative on-premises or managed security service solutions and thus enables the increase of security within an *Identity Federation* without substantially limiting the structural flexibility of related business processes. In reverse, the proposed system contributes to increasing the flexibility of *Federated Business Processes* with pre-specified security and QoA requirements. For further strengthening of the trust chain, end-to-end integrity controls between ASP and SPs were implemented. Hence, the system is subject to two major restrictions: (1) So far, the application is limited to non-mobile use cases since the applied biometric method based on typing is not specifically optimized for the processing of characteristics specific to mobile input devices. However, there is ongoing research in applying keystroke dynamics on touchscreens (see Section 7.) and our systems provides for the supplementation of additional authentication modules. (2) Furthermore, the initial service deployment requires the manual installation of a component connecting the service with the IdPs internal IAM system. This would not be necessary for IAM systems natively supporting the use of external authentication services for functional enhancement.

7. RELATED WORK

SENK proposes a concept for the enforcement of keystroke dynamics-based authentication during the access to physically distributed IT resources (e.g. digital document files) in highly flexible environments [4]. This is based on advanced access control concepts and does not focus on IdM. This paper's proposed system in contrast focuses on the protection of Web-based services within an identity federation and the flexibility of the underlying IdM infrastructure by providing F2A on-demand according to cloud computing principles and here, on the technical implementation of such a system. SENK and DOTZLER evaluate this work's proposed biometric A3S system from a data protection point of view including cloud-specific technical security controls for the protection of infrastructure resources, communication and storage security, and identity and access management. A user-centric Web-based biometric authentication system based on keystroke dynamics and the OpenID protocol is proposed by OLDEN [68]. It focuses on the quality and security problems of such applications. However, this system provides neither for multi-tenancy nor for business administration controls and as such is not applicable for cloud-based service provisioning. Recent work presents substantial improvements in regard to the performance of keystroke dynamics methods, both of fixed text [62, 71] and free text methods [67]. Furthermore, there is numerous current research regarding the enhancement of typing biometrics in mobile applications [75, 76, 77, 78, 65].

8. CONCLUSION

Based on keystroke dynamics a cloud-based authentication system for the enhancement of existing infrastructures for the execution of *Federated Business Processes* was implemented and validated by means of a fictional use case in the context of hBP. Future development should focus on the application of sophisticated controls for cloud data security, the enhancement and standardization of IdM systems for seamless integration of externally provided authentication systems, and the application and validation of the prototype implementation in real world scenarios.

REFERENCES

- [1] L. Boursas, "Trust-based access control in federated environments," Ph.D. dissertation, Techn. Univ, München, 2009.
- [2] W. Hommel, *Architektur- und Werkzeugkonzepte für föderiertes Identitäts-Management*. München: Dr. Hut, 2007.
- [3] M. Menzel, I. Thomas, and M. Meinel, "Security requirements specification in service-oriented business process management," in *Proc. of the International Conference on Availability, Reliability and Security (ARES'09)*, 2009, pp. 41–48.
- [4] C. Senk, "Securing inter-organizational workflows in highly flexible environments through biometrics," in *Proc. of ECIS*, Pretoria, 2010.

- [5] A. Bhargav-Spantzel, A. C. Squicciarini, and E. Bertino, "Trust negotiation in identity management," *IEEE Security & Privacy*, vol. 5., no. 2, pp. 55–63, 2007.
- [6] H. Reiser, *Ein Framework für föderiertes Sicherheitsmanagement*. München: LMU München, 2008.
- [7] E. van Heck and P. Vervest, "Smart business networks: How the network wins," *Communications of the ACM*, vol. 50, no. 6, pp. 28–37, 2007.
- [8] V. Lotz, "Soa-sicherheit für moderne unternehmen – anforderungen an soa-sicherheit auf dem weg zum virtuellen unternehmen," *Datenschutz und Datensicherheit - DuD*, vol. 31, no. 9, pp. 644–647, 2007.
- [9] M. Papazoglou and W.-J. van den Heuvel, "Service oriented architectures: Approaches, technologies and research issues," *The VLDB Journal*, vol. 16, no. 3, pp. 389–415, 2007.
- [10] A. Ghose and G. Koliadis, "Auditing Business Process Compliance," in *Service-Oriented Computing - ICSOC 2007, Fifth International Conference, Vienna, Austria, September 17-20, 2007, Proceedings*, ser. Lecture Notes in Computer Science, Bernd J. Krämer, Kwei-Jay Lin, and Priya Narasimhan, Eds., vol. 4749. Springer, 2007, pp. 169–180.
- [11] S. Goedertier and J. Vanthienen, "Designing Compliant Business Processes with Obligations and Permissions," in *Business Process Management Workshops, BPM 2006 International Workshops, BPD, BPI, ENEI, GPWW, DPM, semantics4ws, Vienna, Austria, September 4-7, 2006, Proceedings*, ser. Lecture Notes in Computer Science, Johann Eder and Schahram Dustdar, Eds., vol. 4103. Springer, 2006, pp. 5–14.
- [12] A. Teubner and T. Feller, "Informationstechnologie, governance und compliance," *Wirtschaftsinformatik*, vol. 50, no. 5, pp. 400–407, 2008.
- [13] D. Wagner, C. Suchan, B. Leunig, , and J. Frank, "Towards the analysis of information systems flexibility: Proposition of a method," in *Wirtschaftsinformatik Proceedings 2011*, 2011, p. Paper 34.
- [14] H. Gomi, "An Authentication Trust Metric for Federated Identity Management Systems," in *Security and Trust Management*, ser. Lecture Notes in Computer Science, J. Cuellar, J. Lopez, G. Barthe, and A. Pretschner, Eds. Springer Berlin / Heidelberg, 2011, vol. 6710, pp. 116–131.
- [15] I. Thomas, M. Menzel, and C. Meinel, "Using quantified trust levels to describe authentication requirements in federated identity management," in *Proceedings of the 2008 ACM Workshop on Secure Web Services*, E. Damiani and S. Proctor, Eds. New York, N.Y: ACM Press, 2008, pp. 71–80.
- [16] C. Senk, "Future of cloud-based services for multi-factor authentication: Results of a delphi study," in *CLOUD-COMP 2012, 3rd International Conference on Cloud Computing, Vienna, Austria, September 24-26, 2012*.
- [17] A. Jain, P. Flynn, and A. Ross, Eds., *Handbook of Biometrics*. New York: Springer, 2007.
- [18] J. A. Pope and D. Bartmann, "Securing online transactions with biometric methods," *International Journal of Electronic Marketing and Retailing*, vol. 3, no. 2, pp. 132–144, 2010.
- [19] Gemalto, "Are cios losing the battle for secure network access?" 2010.
- [20] C. Eckert, *IT-Sicherheit: Konzepte, Verfahren, Protokolle*, 6th ed. München: Oldenbourg, 2009.
- [21] J. Fenn, "Hype cycle for emerging technologies," 2010.
- [22] G. v. Graevenitz, *Erfolgskriterien und Absatzchancen biometrischer Identifikationsverfahren*. Kassel: Lit, 2006.
- [23] B. Furth, "Cloud Computing Fundamentals," in *Handbook of Cloud Computing*, B. Furht and A. Escalante, Eds. Boston, MA: Springer US, 2010, pp. 3–20.
- [24] C. Höfer and G. Karagiannis, "Cloud computing services: taxonomy and comparison," *Journal of Internet Services and Applications*, pp. 1–14, 2011.
- [25] W. Streitberger and A. Ruppel, *Cloud Computing Sicherheit: Schutzziele, Taxonomie, Marktübersicht*. Fraunhofer-Institut für Sichere Informationstechnologie SIT, 2009.
- [26] F. Dotzler, *Datenschutzrechtliche Aspekte und der Einsatz biometrischer Systeme in Unternehmen: Eine exemplarische Betrachtung von Systemen auf der Grundlage des biometrischen Merkmals Tippverhalten*. Köln: Kölner Wissenschaftsverlag, 2010.
- [27] C. Senk and A. Holzapfel, "Market overview of security as a service systems," in *ISSE 2011 Securing Electronic Business Processes*, N. Pohlmann, H. Reimer, and W. Schneider, Eds., 2011.
- [28] R. Dierstein, "Sicherheit in der informationstechnik: Der begriff it-sicherheit," *Informatik Spektrum*, vol. 27, no. 4, pp. 343–353, 2004.
- [29] C. Melzer-Andelberg, *Identity Management. Eine Einführung. Grundlagen, Technik, wirtschaftlicher Nutzen*. Heidelberg: Dpunkt, 2008.
- [30] C. Schläger, *Attribute based infrastructures for authentication and authorisation*, 1st ed. Lohmar and Köln: Eul, 2008.
- [31] Bundesamt für Sicherheit in der Informationstechnik, "Soa-security-kompodium. sicherheit in service-orientierten architekturen: Version 2.0," 2010.
- [32] B. Glade, "Identity assurance framework: Assurance levels," 2009. [On-

- line]. Available: <http://kantarainitiative.org/confluence/download/attachments/38371432/Kantara+IAF-1200-Levels+of+Assurance.pdf>
- [33] E. Bertino, L. Martino, F. Paci, and A. Squicciarrini, *Security for Web Services and Service-Oriented Architectures*. Heidelberg: Springer, 2010.
- [34] N. L. Clarke, *Transparent User Authentication - Biometrics, RFID and Behavioural Profiling*. Springer, 2011.
- [35] N. Cowan, C. C. Morey, Z. Chen, A. L. Gilchrist, and J. S. Sauls, "Theory and Measurement of Working Memory Capacity Limits," ser. *Psychology of Learning and Motivation*, B. H. Ross, Ed. A. Press, 2008, vol. 49, pp. 49–104.
- [36] P. Hoonakker, N. Bornoe, and P. Carayon, "Password Authentication from a Human Factors Perspective: Results of a Survey among End-Users," in *Human Factors and Ergonomics Society 54rd Annual Meeting*. Human Factors and Ergonomics Society, 2009, pp. 459–463.
- [37] R. Oppliger, *Internet and Intranet security*. Boston: Artech House, 1998.
- [38] R. E. Smith, *Authentication: From passwords to public keys*. Boston: Addison-Wesley, 2002.
- [39] L. St. Clair, L. Johansen, W. Enck, M. Pirretti, P. Traynor, and P.-J. T. McDaniel, "Password Exhaustion: Predicting the End of Password Usefulness," in *Information systems security*, A. Bagchi and V. Atluri, Eds. Berlin: Springer, 2006, pp. 37–55.
- [40] M. Weber, *Akzeptanz biometrischer Authentifizierungssysteme*. Mannheim: Universität Mannheim, 2008.
- [41] P. Mell and T. Grance, "The nist definition of cloud computing," *National Institute of Standards and Technology*, vol. 53, no. 6, p. 50, 2009. [Online]. Available: <http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc>
- [42] H. La and S. Kim, "A systematic process for developing high quality saas cloud services," in *Proc. of CloudCom*, Springer, 2009, pp. 278–289.
- [43] T. Mather, S. Kumaraswamy, and S. Latif, *Cloud security and privacy: [an enterprise perspective on risks and compliance]*, 1st ed., ser. *Theory in practice*. Sebastopol, Calif: O'Reilly, 2009.
- [44] W. Sun, K. Zhang, S.-K. Chen, X. Zhang, and H. Liang, "Software as a service: An integration perspective," in *Service-Oriented Computing – ICSOC 2007*, ser. *Lecture Notes in Computer Science*, B. Krämer, K.-J. Lin, and P. Narasimhan, Eds. Springer Berlin / Heidelberg, 2007, vol. 4749, pp. 558–569.
- [45] S. Bajaj, G. Della-Libera, B. Dixon, M. Dusche, M. Hondo, M. Hur, C. Kaler, H. Lockhart, H. Maruyama, A. Nadalin, N. Nagaratnam, A. Nash, H. Prafullchandra, and J. Shewchuk, "Web services federation language (ws-federation): Version 1.0," 2003. [Online]. Available: <http://specs.xmlsoap.org/ws/2003/07/secext/WS-Federation.pdf>
- [46] T. Wisniewski, T. Nadalin, S. Cantor, J. Hodges, and P. Mishra, "Saml v2.0 executive overview," 2005. [Online]. Available: <http://www.oasis-open.org/committees/download.php/13535/sstc-saml-exec-overview-2.0-cd-01-2col.pdf>
- [47] F. Chong and G. Carraro, "Architecture strategies for catching the long tail," 2006.
- [48] J. Kabbeldijk and S. Jansen, "Variability in Multi-tenant Environments: Architectural Design Patterns from Industry," in *Advances in Conceptual Modeling. Recent Developments and New Directions*, ser. *Lecture Notes in Computer Science*, O. d. Troyer, C. Bauzer Medeiros, R. Billen, P. Hallot, A. Simitsis, and H. van Mingroot, Eds. Springer Berlin / Heidelberg, 2011, vol. 6999, pp. 151–160.
- [49] C.-J. Guo, W. Sun, Z.-B. Jiang, Y. Huang, B. Gao, and Z.-H. Wang, "Study of Software as a Service Support Platform for Small and Medium Businesses," in *New Frontiers in Information and Software as Services*, ser. *Lecture Notes in Business Information Processing*, D. Agrawal, K. S. Candan, W.-S. Li, W. Aalst, J. Mylopoulos, M. Rosemann, M. J. Shaw, and C. Szyperski, Eds. Springer Berlin Heidelberg, 2011, vol. 74, pp. 1–30.
- [50] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," *Journal of Network and Computer Applications*, vol. 34, no. 1, pp. 1–11, 2011.
- [51] D. Huang, X. Zhang, M. Kang, and J. Luo, "MobiCloud: Building Secure Cloud Framework for Mobile Computing and Communication," in *Proceedings of the 2010 Fifth IEEE International Symposium on Service Oriented System Engineering*, ser. *SOSE '10*. Washington, DC, USA: IEEE Computer Society, 2010, pp. 27–34.
- [52] S. Lehmann, T. Draisbach, C. Koll, P. Buxmann, and H. Diefenbach, "Saas-preisgestaltung: Bestehende preismodelle im überblick," in *Software-as-a-Service*, A. Benlian, T. Hess, and P. Buxmann, Eds. Gabler, 2010, pp. 155–169.
- [53] P. Buxmann and T. Hess, "Software as a service," *Wirtschaftsinformatik*, vol. 50, no. 6, pp. 500–503, 2008.
- [54] T. Moses, "extensible access control markup language tc v2.0 (xacml)," 2005. [Online]. Available: http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf
- [55] Internet2, "Shibboleth: A project of the internet2 middleware initiative," 2011. [Online]. Available: <http://shibboleth.internet2.edu/>

- [56] R. L. Morgan, S. Cantor, S. Carmody, W. Hoehn, and K. Klingenstein, "Federated security: The shibboleth approach," *EDUCAUSE Quarterly*, vol. 27, no. 4, pp. 12–17, 2004.
- [57] H. Lockhart and B. Campbell, "Security assertion markup language (saml) v2.0 technical overview," 2008. [Online]. Available: <http://www.oasis-open.org/committees/download.php/27819/sstc-saml-tech-overview-2.0-cd-02.pdf>
- [58] T. Dunstone and N. Yager, *Biometric System and Data Analysis: Design, Evaluation, and Data Mining*, 1st ed. Springer Publishing Company, Incorporated, 2008.
- [59] I. Bakdi, *Benutzerauthentifizierung anhand des Tippverhaltens bei Verwendung fester Eingabetexte*. Regensburg: Universitätsverlag, 2007.
- [60] A. Jain and A. Ross, "Introduction to Biometric Recognition," in *Handbook of Biometrics*, A. Jain, P. Flynn, and A. Ross, Eds. New York: Springer, 2007, pp. 1–22.
- [61] D. Bartmann, I. Bakdi, and M. Achatz, "On the design of an authentication system based on keystroke dynamics using a predefined input text," *International Journal of Information Security and Privacy*, vol. 1, no. 2, pp. 1–12, 2007.
- [62] A. Beer, *Optimierung tippverhaltensbasierter, biometrischer Verfahren im Umfeld kurzer Eingabetexte*. Aachen: Shaker, 2012.
- [63] F. Bergando, D. Gunetti, and C. Picardi, "User authentication through keystroke dynamics," *ACM TISSEC*, vol. 5, no. 4, pp. 367–397, 2002.
- [64] F. Monrose and A. D. Rubin, "Keystroke dynamics as a biometric for authentication," *Computers and Security*, vol. 16, no. 4, pp. 351–359, 2000.
- [65] H. Saevanee and P. Bhattarakosol, "Authenticating user using keystroke dynamics and finger pressure," in *Consumer Communications and Networking Conference, 2009. CCNC 2009. 6th IEEE*, jan. 2009, pp. 1–2.
- [66] R. Janakiraman and T. Sim, "Keystroke Dynamics in a General Setting," in *Proc. of ICB*. Springer, 2007, pp. 584–593.
- [67] S. Erdenreich, *Negative Identifizierung anhand des Tippverhaltens bei Verwendung fester und freier Textbestandteile*. Heidelberg: Springer Vieweg, 2012.
- [68] M. Olden, *Biometric authentication and authorisation infrastructures*. Regensburg: Universität Regensburg, 2010.
- [69] Biometric Evaluation Methodology Working Group, "Biometric evaluation methodology," 2002.
- [70] Bundesamt für Sicherheit in der Informationstechnik, "Untersuchung der leistungsfähigkeit von biometrischen verifikationssystemen - biop ii," 2005.
- [71] J. Schenkl, *Tippverhaltenserkennung auf Basis benutzerindividueller, fester Eingabetexte*. Aachen: Shaker, 2012.
- [72] R. Giot, M. El-Abed, and C. Rosenberger, "Keystroke dynamics with low constraints svm based passphrase enrollment," in *Proceedings of the 3rd IEEE international conference on Biometrics: Theory, applications and systems*, ser. BTAS'09. Piscataway, NJ, USA: IEEE Press, 2009, pp. 425–430.
- [73] F. Obergrusberger, B. Baloglu, J. Saenger, and C. Senk, "Biometric identity trust: Toward secure biometric enrollment in web environments," in *CLOUDCOMP 2012, 3rd International Conference on Cloud Computing, Vienna, Austria, September 24-26, 2012*.
- [74] D. Fox, "Zum Problem der Gültigkeitsprüfung von Schlüsselzertifikaten," in *Tagungsband 6. Deutscher IT-Sicherheitskongress des BSI 1999*, Bundesamt für Sicherheit in der Informationstechnik, Ed. Ingelheim: SecuMedia, 1999, pp. 215–230.
- [75] N. Clarke and S. Furnell, "Advanced user authentication for mobile devices," *Computers and Security*, vol. 26, no. 2, pp. 109 – 119, 2007.
- [76] H. Crawford, "Keystroke dynamics: Characteristics and opportunities," in *Privacy Security and Trust (PST), 2010 Eighth Annual International Conference on*, aug. 2010, pp. 205–212.
- [77] S. M. Kolly, R. Wattenhofer, and S. Welten, "A personal touch: recognizing users based on touch screen behavior," in *Proceedings of the Third International Workshop on Sensing Applications on Mobile Phones*, ser. PhoneSense '12. New York, NY, USA: ACM, 2012, pp. 1:1–1:5.
- [78] E. Maiorana, P. Campisi, N. González-Carballo, and A. Neri, "Keystroke dynamics authentication for mobile phones," in *Proceedings of the 2011 ACM Symposium on Applied Computing*, ser. SAC '11. New York, NY, USA: ACM, 2011, pp. 21–26.

BIOGRAPHY OF AUTHORS



Dr. Christian Senk studied business informatics at the University of Regensburg and completed his Ph.D. afterward. Since 2013, he is employed as information security manager.



Florian Obergrusberger studied business informatics at the University of Regensburg and is currently completing a Ph.D. program. Additionally he works as IT project manager.



Prof. Dr. Dieter Bartmann studied mathematics, physics and informatics at the Technical University of Munich. Afterward, he worked as full professor at the universities of Erlangen-Nuremberg, Bamberg, Mannheim, and St. Gallen. In 1993, he took over the management of the chair Business Informatics II at the University of Regensburg. Furthermore he was managing director of ibi research institute and Psylock GmbH. He retired in 2010.
