Multi-Factor Authentication for Public Displays using the Semantic Ambient Media Framework: Interconnecting Semantic Media and Devices

David Bouck-Standen, Josefine Kipke
Kingsbridge Research Center
Glasgow, United Kingdom
email: {dbs, jfk.student}@kingsbridge.eu

Abstract—**In this contribution, we present an approach to encounter various challenges of the growing amount of media available in our digital society as well as an individual's need to access structure and ordered information presents applying the Semantic Ambient Media Framework. The framework extends digital media, devices and applications, as well as services and with digital meta-data, interconnects them through semantic models, and makes them accessible in a Web-based API. In the event the API is accessed, the framework's services tailor the media, depending on context they are used in, their semantic interconnection with other media, and the specific application, device, and context they are accessed from. A possibility to access the information stored within the Semantic Ambient Media Framework is showing media on public displays. In order for public displays to deliver private, personalized, or sensitive contents or provide access to user-specific functionality, authentication mechanisms are required. On public displays, authentication is subject to a number of risks, especially, if displays offer multi-touch interfaces or grow even larger. In this contribution, we present a multi-factor authentication system for public displays using the Semantic Ambient Media Framework. In our approach, no actual credentials have to be typed in on the public display, as this makes use of the users' personal mobile devices and works with a one-time and location-based code. This contribution illustrates the concept and system architecture of the Semantic Ambient Media Framework in a working scenario together with multi-factor authentication for public displays that protects against threads, such as shoulder surfing, thermal attacks, or smudge attacks, which we also illustrate. We conclude with an outline of future work.**

Keywords-Semantic Media; Pervasive Displays; Multi-factor Authentication; Semantic Repository.

I. INTRODUCTION

Feature-rich multimedia systems allow users to produce high amounts of user-generated content. The contexts technology is used in also shift towards mobile and pervasive computing. Today, users use public displays to access public as well as personalized information [1] through interconnected multimedia applications [2]. In order to produce digital media, the users utilize their personal mobile devices equipped with cameras, such as smartphones, tablets, and other devices to interconnect with other systems through the Internet [3], [4].

As each multimedia system uses technologies with different interaction paradigms, they offer different capabilities for presentation, processing, and storing information in their own content repositories [5]. Focusing a vision of a convergence of personal or social information, at least the interconnection of multimedia or media storage systems, or at best a single multi-purpose multimedia repository system would be required [6]. With such a system, media would no longer be isolated for use in a single application or on a single device. Although today Cloud-based solutions already exist, however rather serve the purpose of harvesting data [7], than providing the service described above.

These challenges have been researched in various context-specific domains, as related work (cf. Section II) indicates. With the *Semantic Ambient Media Framework* (SAM.F) [2], this contribution presents a general context-independent approach. SAM.F is a framework that semantically interconnects (a) *digital media*, (b) *devices and applications*, and (c) *services*, which are enriched by digital meta-data in the form of semantic annotations. For both client application development, as well as the extension of framework functionality, SAM.F offers various interfaces for developers.

In SAM.F, digital media consists of, e.g., text, photos, audio, videos, animations, 3D objects, or 3D scenes. These are extended by digital properties, e.g., by classifying the media's content in the internal model of SAM.F. These digital properties include the Meta data extracted from the original file, such as Meta information on MIME type, encoding, or Exif data. For devices, in SAM.F, we model digital properties reflecting, e.g., the devices' capabilities', it's internal hardware, location, capacity, screen size, or screen resolution.

All digital properties are utilized by the services in SAM.F. Client applications running on users' devices access the services of SAM.F through a Web-based API. Each service serves a dedicated purpose, interconnecting devices and applications through the shared use of digital media and services. The service-based architecture of SAM.F is extendable, providing developers with dedicated interfaces and the means to develop new modularized services for SAM.F, as described in detail in this contribution.

In this article, we focus on a working scenario application using SAM.F to provide access to information stored in the framework.

Today, there is a growing number of large multi-touch displays, which are deployed in public spaces, such as public squares, airports, train stations, or in streets or, e.g., museums. These so-called Public displays consist of large multi-touch displays connected to a content providing system, e.g., via the Internet. They offer an entry point for a user to access digital data, such as stored within SAM.F. With the increasing demand for public displays to offer access to personalized or context-specific content or functionalities [8], they offer a supplementary or specialized digital interface device to the users' smartphones or mobile devices that most Internet users possess. Hence, accessing protected data and contexts or user-tailored functionality on public displays presents the need of a secure method for user authentication.

Authentication in general requires a user to enter credentials or use other means for personal identification, only known to or in possession of the user himself. This could be, e.g., classically a username-password combination. More sophisticated methods rely on the uniqueness of a thumbprint, the iris, or other biometrical information unique to the user [9].

The increasing use and functionality of public displays require a solution that protects users and systems against threats. Known threats can be for example *shoulder surfing attacks* (a), where the user is observed while authenticating [10], *thermal attacks* (b), where heat traces resulting from the user's interactions are made visible revealing the sensitive authentication data [11][12], or *smudge attacks* (c) that exploit the residues from finger prints on touch-screens [13]. Research on these techniques indicate that shoulder surfing occurs in daily contexts [10]. All three attack methods have in common that displaying a digital keyboard or using a software keyboard is vulnerable to them. For this reason and to prevent possible attacks exploiting the users' interactions with the systems, systems for biometrical authentication or gaze-touch have been proposed [14], as we explore in related work.

Using additional hardware for public displays, such as bio-scanners or cameras, comes with costs and the need to retrofit most public displays currently deployed. A solution with minimal hardware requirements is more likely to be widely accepted. Thus, one of the challenges of this work is to find a solution that does not require hardware upgrades of public displays.

Modern smartphones are personal devices equipped with different sensors and mostly at least one camera. The smartphone is still on the rise in 2020 due to its multi-functionality and connectivity, as almost 8 out of 10 Internet users in the EU surfed via a mobile or smartphone. The trend toward mobile technology and mobile Internet usage can still be observed globally [15].

In this work, we present a technical solution we developed as a prototype at the Kingsbridge Research Center (KRC), which addresses these challenges with a minimal technical solution. This makes use of a *multi-factor authentication* (MFA) [1]: The first factor is the *ownership* (i) of a personal mobile device, such as a smartphone. The second factor is *knowledge* (ii) of personal credentials, such as the combination of username and password. Using GPS data, we also use the user's and display's *location* (iii) as third factor.

The concept of this work makes use of the interconnection of the devices through the Internet, using the Semantic Ambient Media Framework (SAM.F) [2] as an authoritative facilitator between smartphones and public displays.

In this contribution, we regard related work in Section II, and present a practical scenario in Section III. In Section IV, we outline the system concept and architecture and describe our prototype implementation. In the final section, we summarize our work and illustrate future work.

II. Related Work

Semantic media comprises the integration of data, information and knowledge. This relates to the Semantic Web [16] and aims at allowing computer systems as well as humans to make sense of data found on the Web. This research field is of core interest since it yields naturally structured data about the world in a well-defined, reusable, and contextualized manner.

The field of metadata-driven digital media repositories is related to this work [17] as well. Apart from the goals of delivering improved search results with the help of Meta information or even a semantic schema, SAM.F distinguishes itself from a pure repository by containing and using multiple repositories as internal components, as illustrated below. As Sikos [18] observes, semantic annotations feature unstructured, semi-structured, or structured media correlations. Sikos outlines the lack of structured annotation software, in particular with regard to generating semantic annotations for video clips automatically. SAM.F offers means for both structured and semi-structured semantic annotations. Through an interface, the functionality of SAM.F can be extended to, e.g., automatically annotate media as outlined below, but is not limited to video clips. By these means, SAM.F delivers even more sophisticated features.

In general, SAM.F facilitates collecting, consuming and structuring information through device-independent interaction with semantically annotated media, whereas the linked data research targets sharing and connecting data, information and knowledge on the Web [19]. The concept originally developed by the author [20] was already used in different contexts, e.g., the automatic reconstruction of 3D objects from photo and video footage [2].

Blumenstein et al. [21] outline a technical concept in museum context, that relies on a server-based architecture to provide museum content in a multi-device ecology. SAM.F could be used in similar contexts, as the scenario outlines in Section III, but is not limited to the use in museums.

Ambient systems can provide a platform for displaying of and interaction with media [22]. In this context, the delivery of content on different devices is an important issue in SAM.F, e.g., with respect to the devices' capabilities or their context of use, and SAM.F addresses this challenge by provisioning digital media depending on applications and devices specifications or capabilities. SAM.F also addresses the issue of limited bandwidth of mobile devices.

The Social Web is related to this work, as it makes it easy for people to publish media online. Yadav et al. [23] propose a framework interconnecting Social Web and Semantic Web by semantically annotating and structuring information people share. SAM.F could be used in this way, but focuses on semantically enriched or described instances of media, devices and services.

Semantic frameworks are used in various contexts, such as multimodal representation learning, as proposed by Wang et al. [24]. In their approach, Wang et al. use a deep neural framework to capture the high-level semantic correlations across modalities, which distinguishes this approach from SAM.F.

This work also takes place in the research field of public displays. Related work indicates a general increase in the deployment of public displays [25].

Today, public displays are widely connected in client-server-applications for content serving purposes, and they are connected through the Internet [25]. For example, Memarovic et al. focus on interconnecting displays, e.g., with social media [26]. Our work ties onto related work through its modular client-server-based architecture. As this work depends on Web-based and modular technology, it can be integrated into other existing projects.

The field of multi-factor authentication (MFA) is an important research field for this work. As Ometov et al. [9] recently surveyed state of the art methods for MFA, illustrate technical requirements, and identify commercial, governmental, and forensic applications as three market-related groups of applications for MFA. In context with public displays, this work can potentially be deployed in all three fields, but according to Ometov et al. the use in commercial applications is most likely.

One of the main challenges of MFA is the absence of a correlation between the user identity and the identities of smart sensors and systems or devices, as Ometov et al. observe [9]. Ometov et al. propose a user-friendly process to establish a trust relationship to gain access rights, whereas Mannan et al. [27] propose a concept to use a personal device to strengthen password authentication from untrusted computers. We combine aspects from these theoretical approaches to our technically limited setting, as outlined above, and present a feasible solution for the MFA for public displays using SAM.F.

With the system called Tacita, Shaw et al. [25] demonstrate a system to personalize public display experience by utilizing proximity detection for user's mobile devices, e.g., with iBeacon technology.

Tacita ubiquitously personalizes public displays' content, whereas GTmoPass proposed by Khamis et al. relies on gaze-touch detection through the smartphone and the identification of the display via a Bluetooth Low Energy (BLE) beacon [14].

These approaches are distinguished from the approach presented in this contribution, as the system we develop directly authenticates users and requires a direct user interaction on the public display. It therefore supports direct use, which features the use of public displays in both unauthenticated, as well as authenticated contexts, especially, if personalized or personal information is displayed or the public display is used to access sensitive functionality. In addition, the solution proposed in this article does not require any supplementary hardware, such as BLE beacons or cameras.

The following section illustrates the system's concept and architecture.

III. A PRACTICAL SCENARIO

Together with our project partner, the *Audiovisual Archive of German-language Literature e.V.* in the Hanseatic City of Bremen, Germany, we develop a scenario to add a digital information meta-layer to a physical exhibition planned in a cultural centre in Bremen.

The scenario illustrates both the use of the Semantic Ambient Media Framework (SAM.F) together with the multi-factor authentication for public displays (MFA4PD), which are illustrated in detail in this contribution. This exemplary use-case focuses on the practical implementation. The visualization of information retrieved from SAM.F described in this scenario is not part of our current work. We are planning to contribute this in the future, as it serves for illustration purposes in this article, only.

Emily Walden is 16 years old and is visiting her grandfather Erik Braun in the Hanseatic city of Bremen this weekend. Since she has grown up with technology, Emily is very tech-savvy, while her grandfather owns a smartphone, but only for making phone calls and prefers not to use it at all. He only has little technical affinity.

Erik Braun is interested in literature, while Emily is less enthusiastic about them. Erik Braun became aware of a newspaper article at the cultural centre of the Audiovisual Archive of German-language Literature e.V. in Bremen, which he would like to visit with his granddaughter. That's why he plans their joint excursion through the city so that they will pass by the cultural centre.

After breakfast they start and in the early afternoon arrive at the cultural centre. Through the high glass facade, some exhibits can already be seen, as well as displays on the walls displaying "Literature and I" in large fonts. More as a favour to her grandfather, Emily agrees to a visit and both enter the exhibition, which at this time is especially dedicated to the writers and Nobel-prize winner Günter Grass.

Inside the exhibition, Emily and her grandfather Erik notice a standing desk. She approaches this and learns that this was Grass's standing desk, on which he wrote "The Tin Drum" during his time in Paris. A tablet installed on the standing desk shows a short video, after which the display changes and shows a graph. The graph shows images of the backyard with the entrance to the boiler room, in which Grass wrote the novel. The images are connected by a line to a node with the name "Paris". The node is connected to the node "Günter Grass". Erik and Emily look at the visualization and Emily notices another line connecting the node to a film adaptation of Volker Schlöndorff's Tin Drum. She didn't know there was a film, and she would also watch it with her grandfather instead of reading the book, she joked.

Together they continue through the exhibition and head towards one of the large screens, on which the lettering "Literature and I" is shown. As they approached the display, the wording changes to: "What moves you spontaneously?". Below, they both see various icons displayed below.

Erik, who is a little more reserved than Emily, leaves her to operate the device and watches, as she interacts with the multi-touch display. Spontaneously, she chooses a pictogram with a cooking pot with a trowel.

Immediately the presentation changes and they again see a graph, they recognize from the standing desk. This time, however, Emily notes that the information displayed has to do with cooking. Grandfather Erik, who read Grass but had not yet noticed that the literate had dealt so comprehensively and repeatedly with the topic of hunger and cooking, is also astonished.

On the display, Emily notices a textual hint that tells her, that she can continue exploring the information more deeply from home. She follows the instructions displayed and connects to the Wi-Fi “KulturzentrumBremen” on her Android device. A notification shows up and she opens the mobile’s browser, where she completes a short sign-up form in just a few seconds and is signed-in automatically.

Afterwards, she sees a code with five symbols displayed on her smartphone. On the display, Emily selects the symbols shown on her smartphone from a grid of nine symbols shown on the display. The display now indicates that Emily has to check her smartphone again. On the smartphone, a prompt is displayed and Emily confirms, that she wants to log in on a display named “Kulturzentrum Bremen - Bildschirm 4”. She quickly cross-checks the name of the display she and her grandfather are standing in front of and confirms the login on her smartphone.

The display immediately changes from the login mask back to the graph and greets Emily with her name. Emily now sees that she can bookmark nodes by selecting them. During their exploration.

Emily, who is interested in politics, touches a node with the description “Victory over the hunger of the world”. The depiction changes and shows a video in which the writer Günter Grass made a political statement. Emily immediately notices that this was part of a lengthy interview, knowing the digital video controls from social media, and touches the bookmark icon on the screen.

Together with her grandfather, Emily continues to explore the physical and the digital exhibition. Whenever she finds a medium that is interesting, she stores a digital bookmark.

A few days later, Emily already is back with her parents', the ticket of the cultural center in Bremen falls into her hands while she looks through her receipts in her wallet. She discovers a web link on the ticket and opens it in her web browser. After signing in with her credentials she set up during her visit to the cultural center in Bremen, she again sees the graph view and notices an interconnection between nodes that are familiar. In addition to the bookmarks she recognizes, she sees other nodes connected displaying media associated with the topics at hand.

In the following section, we focus on the system concept and architecture.

IV. System Concept and Architecture

In this section, we illustrate the system concept and architecture of SAM.F. Subsequently, based on the framework, we outline the concept and implementation of multi-factor authentication for public displays.

A. The Semantic Ambient Media Framework

SAM.F is a smart media environment, which provides a device-independent access to and interaction with media through devices and applications.

The system’s architecture of SAM.F is based on a system concept following these three considerations:

1. Web-based access provides platform-independent use of the services and access to media inside SAM.F and its repositories from the users’ devices and applications.
2. a service-based modular architecture features extendibility, which provides developers with a framework to develop their own applications, which can be based on or reference to existing services within SAM.F.
3. the concept of Semantic Media regards media independently of their encoding or modality and automatically transcodes or converts media, where necessary and possible, to meet contexts, applications, and devices specifications or criteria.

In the following sections, we focus on the concept of Semantic Media fundamental to SAM.F. We illustrate the system’s architecture and the service concept of SAM.F. Following, the application and device-specific media provisioning is outlined. In addition, technical details on the current implementation of SAM.F are given.

1) Semantic Media

In SAM.F, apart from services delivering media, media themselves are central. Semantic Media consist of plain media, such as text, audio, video, pictures, and 3D media, which are enriched by a dynamic set of semantic annotations. Together, plain media and semantic annotations form *Semantic Media* in SAM.F.

The dynamic set of semantic annotations stored in SAM.F for each media element consist of:

- the original Meta-data of the plain media file. For example, for photos taken with digital cameras, metadata usually contains information on the picture’s location, and camera data such as camera make and model, or camera settings, such as camera capture settings. This data might be useful for SAM.F services and adding it to the set of annotations improves accessibility and performance when further processing media.
- data received from automated algorithms. Pictures for example are submitted to a Computer Vision algorithm by SAM.F automatically and in a background process in order to determine semantic annotations describing the media’s content.
- data received from client applications. As the main user interaction with media through SAM.F is carried out through client applications, in which the context of use is known, this information is stored in additional semantic annotations. This information is collected automatically in a background process through the use of the SAM.F API Web Services, which implicitly reveal the context of use.
- data received from manual user interactions, such as manual annotations or correcting automatic annotations.

It should be noted that the semantic annotations of Semantic Media may not be complete or available for each media element at all times. This is, e.g., due to the context the media is created in, a foreign source the media is accessed from, or incomplete data entered by the user [28]. This observation presents a challenge we discuss at the end of Section IV in terms of the prototype implementation.

The set of annotations described above is not final and can be extended in context of client applications, devices or services.

In SAM.F, the complete set of semantic annotations are abstracted into the Data Model (see Figure 1) in order to be (i) accessible for all services running inside the framework and (ii) accessible independently of the underlying media repository in the Datastore layer (see Figure 1).

Not all annotations are made available for every client application or device through the API Web Services (see Figure 1), as the API Client Model only contains those properties that are required in the corresponding context. This way, overhead in the access of media through client applications is assumed to be significantly reduced. The effects on performance or bandwidth have however not been measured as part of this work. However, we discuss possible issues arising from this approach at the end of Section IV.

It is one of the hypotheses of this work that the quality of semantic annotations as well as the interconnection of media will be a key issue for realizing appealing scenarios using SAM.F, as, e.g., described in the final section of this article. An approach to achieve this is to gather additional sematic annotations through automated algorithms. As illustrated in Figure 2 and mentioned above, pictures, for example, are submitted to a Computer Vision algorithm. In the current implementation, SAM.F interfaces with Microsoft Cognitive Services. Thus, in the background, SAM.F computes additional semantic annotations, which are then stored in the internal Datastore (see Figures 1 and 2).

2) *System Architecture*

The architecture of SAM.F consists of a layer-based system concept, as illustrated in Figure 1. Client applications and devices utilized by users connect to the SAM.F *API Web Services* through the *API Security Layer* via the Internet in order to access media stored in SAM.F or interact with services in the *Service Layer* (see Figure 1).

When interacting with SAM.F, client applications as well as devices exchange information with the framework (see Figure 2) using a defined data model. Thus, for any context, the *API Client Model* can be extended to exactly match the needs of the application, device, or context, if necessary. API Web Services offer access to dedicated services provided by SAM.F, as the scenario described above outlines. Internally, SAM.F works with a dedicated *Data Model*, as illustrated in Figure 1. Any data is mapped from the *Datastore*, which includes external (semantic) databases as well as binary data stores, to the internal Data Model, which applies a homogenous model to potentially heterogenic data. Thus, SAM.F features the integration of different repositories and provides a combined access to Semantic Media. For simplification purposes, and in order to reduce the learning curve when implementing client applications accessing SAM.F, the internal Data Model is only used in the *Provider Layer*, which contains, e.g., authentication or data providers to be accessed by the upper Service Layer, and in the *Service Layer*, as shown in Figure 1. Any Semantic Media, together with semantic annotations, provided by a service to a client is mapped to the specific API Client Data Model, as outlined above, and being served through the API Web Services and the API Security Layer to the client application (see Figure 2).

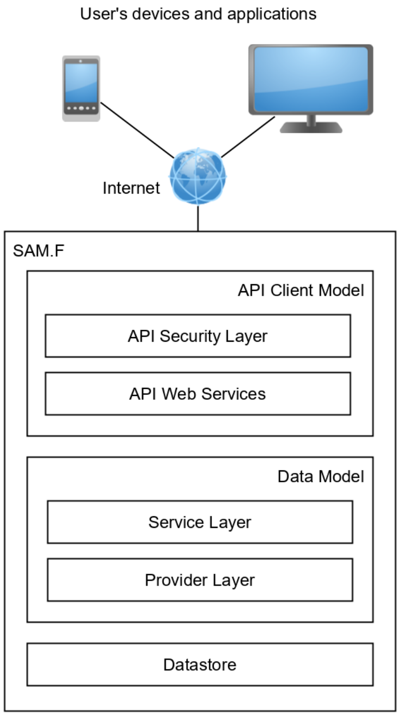


Figure 1: Layered architecture of SAM.F.

With the Data Model only used internally, SAM.F accommodates different models used when storing media in digital repositories. A museum database for example differs significantly from, e.g., the DbPedia's semantic database. To be able to use heterogenous sources simultaneously, different data models are homogenized though the Data Model in SAM.F: by applying the data mapping techniques, the framework uses its own model internally, into which all other models are mapped. Applying data mapping in SAM.F produces constant overhead. However, services and applications, as well as their developers, benefit from only working with data models that are specific to the requirements of the services' or applications' context. This also reduces overhead when loading large sets of Semantic Media.

The range of functions of SAM.F is defined by the functionality provided by services residing in the Service Layer, as illustrated in Figure 1. In the scenario outlined below the developers extend SAM.F by implementing a custom service in order to realize the desired functionality. Thus, in the next section, the SAM.F services are regarded.

3) *SAM.F Services*

Following the implementation principles of SAM.F, a service features a dedicated set of functions in order to provide a certain functionality, e.g., for a use-case or scenario, as outlined above.

Utilizing the Data Model, through the Provider Layer, any service might access Semantic Media from the repositories included in SAM.F's Datastore layer. As a result, services may interchange information in a well-defined context.

SAM.F comes with a set of services that are useful to the developer in a Web-based environment and for developing applications in context of mobile use and the use of Semantic Media, explained in more detail below. In this article, we focus on the basic features the SAM.F services consist of:

- an authentication service to identify and authenticate sessions of applications, devices and users.
- a general media service that allows to retrieve or modify Semantic Media elements for a given keyword in a given general context. Media is retrieved both from the internal datastore, as well as external semantic databases housed in the Datastore layer (see Figure 1) and made available through SAM.F.
- the *Application and Device-specific Media Provisioning* (ADMP) service, which transcodes media based on different settings on client retrieval, as outlined below.

In the scenario outlined above, the developers extend the Service Layer of SAM.F (see Figure 1) and add their service to authenticate users on public displays. This service utilizes the modularized architecture of SAM.F and interfaces with the adjacent upper and lower layers. It also makes use of the default user authentication service. Service execution may either be triggered (i) on demand per request, or (ii) internally. This allows services of SAM.F to automatically run in the background without the necessity of user interactions.

4) *Application and Device-specific Media Provisioning*

Semantic Media in SAM.F can contain various types of plain media. However, their use is determined by the client applications. The devices running these applications are usually limited in their capabilities.

To address these challenges, SAM.F offers an *Application and Device-specific Media Provisioning* (ADMP) for any Semantic Media element retrieved through the API Web Services layer (see Figures 1 and 2).

In general, ADMP transcodes or converts Semantic Media due to specifications given. Trivial examples are the conversion of large photos into thumbnails, including cutting and cropping, if necessary.

ADMP is designed to work in two ways:

- on a per-request basis, in which the application submits the desired parameters (e.g., format, encoding, size, resolution) with every request, or
- on an application or device capability basis. As devices and applications are also represented in the Data Model (see Figure 1) of SAM.F, their capabilities are known to SAM.F. Thus, using per-request parameters can be omitted, if application or device capabilities can be generally set or are valid for multiple requests.

Especially in context of the Web-use of SAM.F and the heterogeneity of devices potentially accessing SAM.F, ADMP's usefulness can be illustrated through these examples, in which the correct parameter settings are

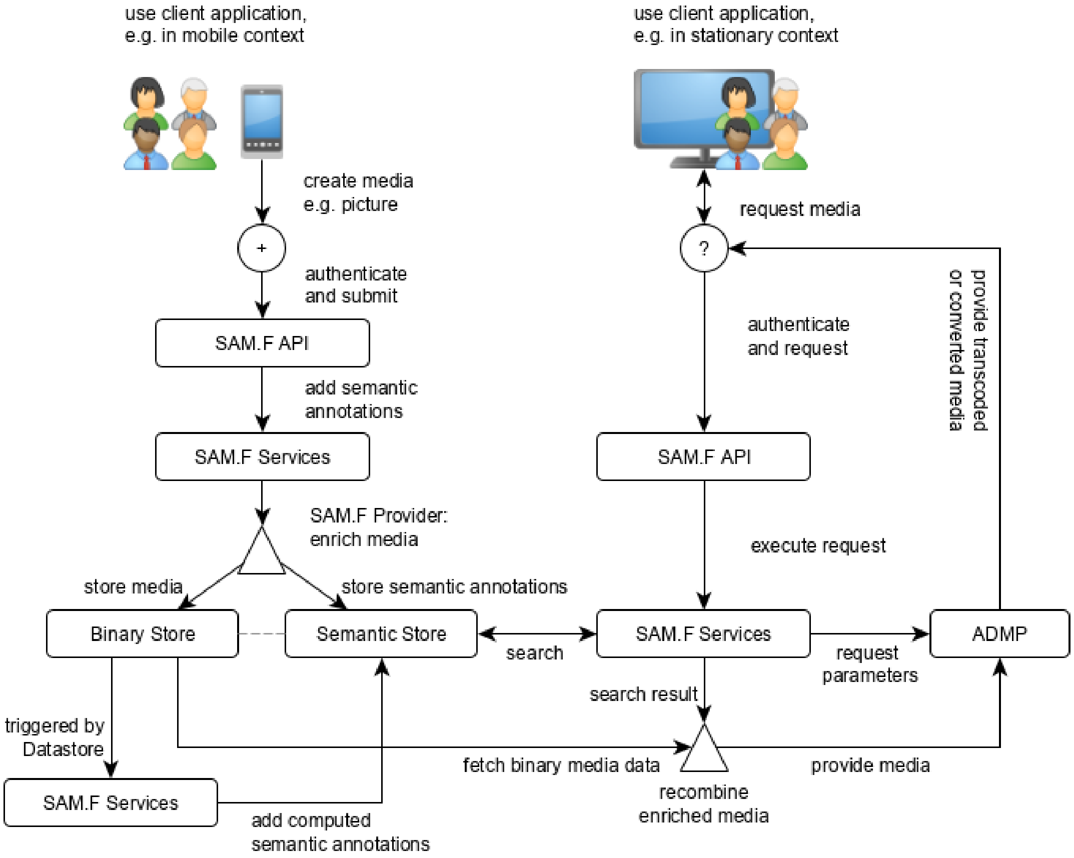


Figure 2: Media creation, enrichment through semantic annotations and retrieval. The Datastore consists of both Binary Store and Semantic Store.

presupposed: A video can be retrieved in different encodings or in matching screen size for the device's resolution. For example, ADMP can provide just the audio track of the video or just the textual transcript. The transcript can also be used to subtitle the video. More challenging 3D objects, which may not be viewed on any device, can be retrieved as a video of the 3D object rotating around the y-axis, or just as a picture in the form of a screenshot of the 3D object.

Reviewing key event-based multimedia applications, Tzelepis et al. [29] observe an enormous potential for exploiting new information sources by, e.g., semantically encoding relationships of different informational modalities, such as visual-audio-text. SAM.F provides these means by transcoding and converting Semantic Media in the background by automated processes.

As a side-effect, using ADMP reduces the use of bandwidth, which is of special interest in mobile contexts.

As these examples indicate, this way of provisioning media though SAM.F provides the means for a vast amount of use-cases. However, the author admits that not all possibilities have been implemented. The ADMP module, which also extends the Service Layer (see Figure 2), can be expanded, as it features an interface with an extendable list of parameters.

5) *Prototype Realization of SAM.F*

A first prototype implementation of SAM.F has been realized at the *Kingsbridge Research Center* (KRC). On the basis of a Windows Server system and its Internet Information Services (IIS) Web server, SAM.F is implemented in C# and runs as IIS Web application. Web services are provided using the Active Server Method File (ASMX) technology.

SAM.F uses an internal database to store all semantic data and semantic correlations. Currently, we follow two main approaches for storage of semantic data.

a) *Working prototype approach*

In our stable prototype approach, semantic annotations used in SAM.F are represented as RDF triples. For performance reasons analyzed under laboratory conditions in experimental settings, SAM.F's internally used RDF data is stored in a NoSQL database, although quantitative performance measurements are future work. SAM.F is compatible to semantic media repositories, e.g., using SPARQL to execute queries. Additionally, other required annotations for external media are stored in the internal datastore of SAM.F. In these terms, external media are media that are made available through SAM.F, but are stored in semantic datastores that are not managed by, but connected to SAM.F.

The approach of combining the automated enhancement of semantic annotations for media and delivering media in a device- or context-specific modality or encoding presents a technical novelty and distinguishes SAM.F from other media frameworks or repositories.

The current prototype has been validated under laboratory conditions. Computations are implemented to be carried out in a complexity of *O(n)*.

Together with our project partner, as outlined below in more detail, we will integrate SAM.F for use in context of research and cultural projects. This will provide the opportunity to evaluate the system under real conditions with regard to functionality and performance.

b) *Experimental approach*

In order to be able to serve client applications connected to the SAM.F API, as depicted in Figure 1, before exposing any information through the API it is mapped into the API Client Model. This well-defined model exposes only those attributes necessary for the given service or context. Thus, a developer can interface an application with SAM.F without prior knowledge of the internal semantic model, or any model applied to a semantic database that might be connected to SAM.F, as outlined in terms of 'external media' in the section above.

Although this approach features a preferable learning curve for developers, it limits the API's capabilities to the information modeled within the API Client Model. It also requires the semantic model to be preset within the implementation of SAM.F.

In our new, highly experimental approach, we are currently implementing an interface that allows the specification of SAM.F's internal model through JSON. Thus, the developer of a client application defines his required model in one or more JSON files, as outlined in Figure 3. From this definition file, SAM.F derives the semantic correlations into an RDF triples, as it sets up the internal model to the developers' specifications.

With the new approach developers are enabled to define their own models, correlations and contexts. However, this is still under research and developers are required to have more understanding of the Semantic Web and semantic queries. We chose JSON notation as shown in Figure 3 because the syntax

```
{
  "properties": {
    "title": {                            <root, properties, title>
      "type": "string",                   <title, type, string>
      "writeable": true                   <title, writeable, true>
    },                                    <root, properties, oncatalogue>
    "oncatalogue": "boolean"              <oncatalogue, type, boolean>
  }
}
```

Figure 3: Basic example for the experimental JSON to RDF conversion.

is more comparable to class modelling, than specifying RDF schema.

We are planning on making this experimental feature available in the future and carry out specific user research with the user group of developers in order to evaluate this highly experimental approach.

6) Summary

SAM.F provides Web-based access for devices and applications and features a service-based architecture, which allows for interaction with media, such as, e.g., text, pictures, audio, video, 3D objects, or 3D scenes.

B. Multi-Factor Authentication for Public Displays

For this approach and under consideration of the technical limitations outlined above, the following is the starting point for this work:

- users are in possession of a smartphone or equivalent device connected to the Internet. They have already registered an account with credentials known to SAM.F beforehand, as this is a preliminary requirement of this work.
- public displays are connected to the Internet and run on Web-based technology, e.g., showing Web-based contents in a browser-based system.
- the user sojourns in the vicinity of a public display and intentionally starts a private context.

Figure 4 illustrates the system's architecture and the starting point. In a single location, one or more users and one or more displays can be present. A user interacts with a single display and is in possession of a personal mobile device, as depicted in Figure 4. All public displays and user's devices are connected to SAM.F through the internet. However, a direct connection between a smartphone and any public display does not exist.

Inside SAM.F, the *multi-factor authentication for public displays* (MFA4PD) module is hosted. Public displays and user's devices connect to the MFA4PD module through the Internet. In addition, public displays connect to external content providers, which are not illustrated in Figure 4, for simplification purposes.

The system's architecture benefits from the technical limitations outlined above. As there is no direct connection necessary between the personal mobile device of a user and the public display used for authentication, there is no need for the display provider to open up his network for foreign devices. Thus, a multi-device ecology within the network of the display provider is not required, resulting in less administrative effort. Whenever an Internet connection has to be provided, e.g., in the event of poor LTE or cellular reception, provisioning a public hotspot is sufficient.

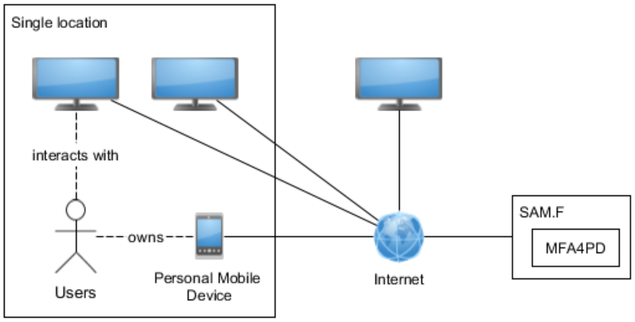


Figure 4. Illustration of the system's architecture and network.

From Figure 4, it can also be observed that no additional hardware, such as, e.g., BLE beacons, is required.

The system concept relies on the interconnection of mobile devices and public displays through SAM.F, which is outlined in the following section.

1) Interfacing MFA with SAM.F Services

The architecture of SAM.F, although described here only with reference to the MFA4PD module, consists of a layer-based system concept, as illustrated in Figure 5. A client application, such as the display or mobile application of this work described in more detail below, connect to the SAM.F *API Web Services* through the *API Security Layer*. Data is exchanged between applications and services, which reside in the *Service Logic* layer, in the form provided by the specification of the *API Client Data Model*. Internally, SAM.F works with a dedicated *Data Model*, as illustrated in Figure 5. Any data is mapped from the *Datastore*, which includes external (semantic) databases, as well as binary data stores, to the internal Data Model, which applies a homogenous model to potentially heterogenic data. For simplification purposes, and in order to reduce the learning curve when implementing applications accessing SAM.F, the internal Data Model is only used in the *Provider Layer*, which contains, e.g., authentication or data providers to be accessed by the upper Service Layer, and in the Service Layer, as shown in Figure 5. Any data provided by a service to a client is mapped to the specific API Client Data Model before being served through the API Web Services and the API Security Layer.

Applying data mapping in SAM.F produces constant overhead, but services and applications, as well as their developers, benefit from only working with data models that are specific to the requirements of the services' or applications' context, reducing overhead when loading large sets of data. Data in this respect describes media, devices and services.

In context of this work, SAM.F serves as authentication provider, which validates user credentials via its standard user service. This work extends the Service Layer of SAM.F by adding the MFA4PD module, which implements the authentication process described in the following section.

2) Authentication Process

To start a private session on one of the public displays, the user opens up the *mobile application* of MFA4PD on his personal smartphone. The user then enters his credentials previously registered with SAM.F, which the Web application submits to MFA4PD, as illustrated in Figure 5.

At this point, the process of authentication might be enhanced by further means of MFA, such as gathering biometrical data from fingerprint sensors, facial recognition, or voice sensors. These extensions however might require at least a hybrid application deployment for mobile devices, in order to access the appropriate sensor data. For this reason, in this initial approach, we focused on the Web application combining MFA with ownership and knowledge factors.

The users are identified and authenticated by MFA4PD through their credentials. During the entire process, MFA4PD continues to check the actual location of the user. The location is determined from the GPS data, which is accessible through the smartphone's Web browser API. If any location mismatch occurs, the process to establish a secure session or the session itself will be terminated immediately for security reasons. This feature might prove useful, whenever a user leaves the location of a public display. However, we did not evaluate this feature's aspect nor the accuracy required from GPS data in order to work in an everyday scenario, yet.

After the user's location and credentials are validated, SAM.F generates a code consisting of five symbols, which is shown to the user on his mobile device, as illustrated in Figure 5. The code is valid for a short period of time and the specific user only.

In order to authenticate him- or herself on a public display, the user has to enter the one-time code shown on his smartphone (Figure 6, please see next page). The user opens up the login dialogue of the *display application* on the public display, and a grid of symbols is displayed. Within this grid, the user now selects the symbols shown on his or her smartphone. The display application communicates the code back to the MFA4PD module, as shown in Figure 5. This serves two purposes:

a. to identify the display, the user selected from the number of public displays available, and
b. to identify the user, who chose a public display.

However, the session is not yet usable. The last step to enable the session on the public display requires the user to again interact with his smartphone in using the *confirm mechanism*. As illustrated in Figure 5, the MFA4PD module sends an authentication request to the mobile application. The dialogue shown indicates a login event took place, together with the name and location shown on the public display. Without the user confirming the login on the mobile device, the session will not be unlocked. The confirmation screen on the smartphone is illustrated in Figure 7.

The users can now put their smartphones away and start using the public display, until they log out.

An additional timeout mechanism prevents misuse of the session on a public display.

The users can also close the session at any time using their mobile devices, e.g., in case they forgot to select the logout function on the public display. In addition, SAM.F monitors the users' location throughout the entire process and session in order to prohibit misuse of login or automatically logout a session after a user clearly left the screen's location.

Now that the system's architecture and concept have been illustrated, in the following section, this approach is viewed with regard to security.

3) Prototype Realization

The prototype consists of three components: (1) the MFA4PD module extending the services of SAM.F, (2) the mobile application and (3) the display application.

SAM.F is developed as Internet Information Services (IIS) application for Windows Servers, as outlined above. The MFA4PD module is implemented as ASMX Web service and a backend-only application, which adds an ASMX Web service to the framework and interfaces with SAM.F.

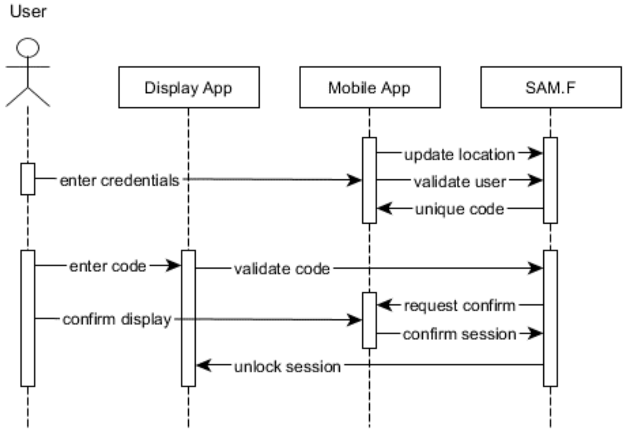


Figure 5. Sequence diagram showing the authentication of one session by a user.

In our initial approach [1] we developed the mobile application as an IIS Web application, which interfaces with the MFA4PD service in order to realize the multi-factor authentication for public displays using SAM.F. It consists from an ASPX form using JavaScript and AJAX to interact with the frameworks service, whereas the graphical user interface can be customized using HTML and CSS. Figure 6 and Figure 7 show the Web application on an Android smartphone.

The display application consists of a graphical component including the necessary HTML, CSS and JavaScript code. It interfaces with the MFA4PD module via JavaScript through AJAX. The display application also comes with a lightweight backend for session management, that also interfaces with the MFA4PD module. This is currently implemented in ASP.NET.

In order to incorporate the display application into an existing application, we provide code snippets that can be integrated into any application. If a target project does not run ASP.NET, the required server-side code can be translated for other frameworks.

In our current approach, we develop a mobile application using Xamarin in addition to the Web application described above, currently focusing on Android devices. Thus, authenticating the mobile application against the SAM.F API is now implemented using token-based authentication. This way, the device ownership factor is strengthened and the session is bound to the user's physical device. In addition, the mobile application can receive push notifications from SAM.F using SignalR, e.g., in order to signal a logout event from a public display directly.

The new mobile application now offers access to the smartphone's sensors. This means although the GPS accuracy and indoor location issues remain analogues to the Web application, the mobile application is now capable of detecting the user's steps. It is our current hypothesis that this can enhance detecting whether a user has left the location of a public display. This is important, e.g., in case a user forgot to logout of his authenticated session on the public display.

The main interface of the Xamarin application with the MFA4PD service is developed as separate Portable Code Library (PCL). Thus, other applications might incorporate public display authentication mechanisms into their own program logic by using the PCL.

We plan to make the prototype available for non-commercial use later this year.

4) Security

As outlined above, related work identifies possible means to attack public display authentication, such as shoulder surfing attacks (a), thermal attacks (b), or smudge attacks (c). In the following, we focus on these client-side attacks.

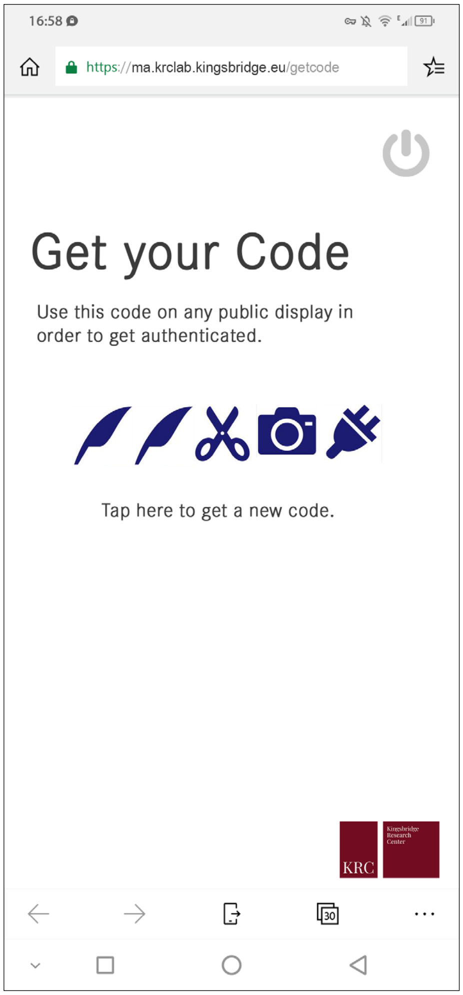
a) Client-side security

Combining ownership and knowledge factors together with the confirm mechanism, only initially entering the user credentials on the mobile application is vulnerable to shoulder surfing attacks. However, once the trust relationship is established between SAM.F and the users' smartphone for the current location, another mobile application login is prohibited for the duration of that trust membership.

In our initial prototype, we use session cookies and device cookies to temporarily store trust relationship data. Device cookies may be subject to manipulation, but session cookies stored on the server would require the attacker to have server access.

We also plan to use the user's location to limit the list of displays he might login-to to the number of displays that actually are in the user's vicinity.

With regard to the one-time code displayed on the mobile application, as well as the user's input of this code on the display application, they are not vulnerable to shoulder surfing attacks. Again, the confirmation mechanism protects the theft of the session. If any irregularity occurs, the user just declines unlocking the session and generates a new code.

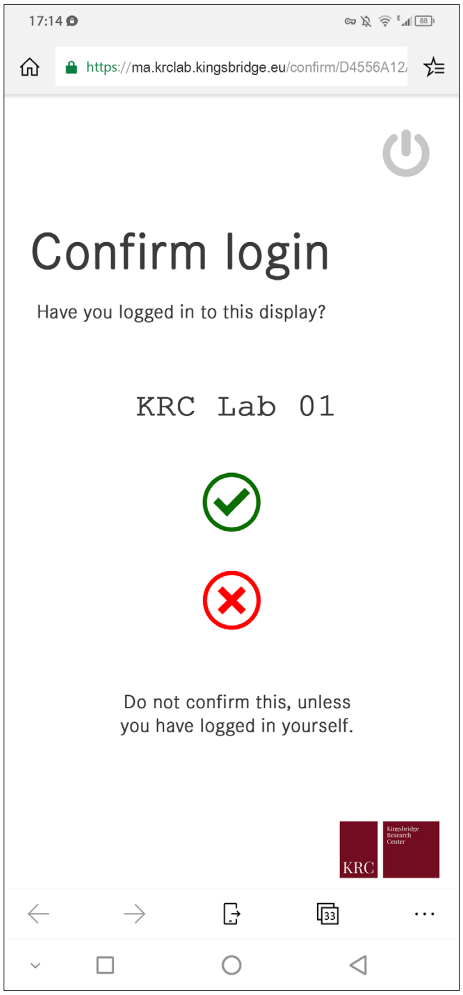

16:58
https://ma.krclab.kingsbridge.eu/getcode
KRC
Kingsbridge Research Center

Get your Code

Use this code on any public display in order to get authenticated.

Tap here to get a new code.

Figure 6. Screenshot taken from an Android 9 smartphone running MFA4PD Web application inside Edge browser. The symbol code displayed authenticates the user on the public display.


17:14
https://ma.krclab.kingsbridge.eu/confirm/D4556A12
KRC
Kingsbridge Research Center

Confirm login

Have you logged in to this display?

KRC Lab 01

Do not confirm this, unless you have logged in yourself.

Figure 7. Screenshot taken from an Android 9 smartphone running MFA4PD Web application inside Edge browser. The login confirmation screen shows up after entering the code on the public display.

If a user accidentally confirms a session on his mobile application for a code that was used on another display or by somebody else, the simplest way is to just close the session from the user's smartphone immediately. However, this case is unlikely to occur due to the one-time code concept and the narrow time frame, in which a code can be used.

Both thermal attacks and smudge attacks cannot be used on public displays in this approach. Once the one-time code has been used, it is invalidated. The statistical possibility of guessing a one-time code can be decreased by a higher number of symbols used in the one-code, a larger symbol inventory, or a larger grid.

During the entire login process and, in concept, during the entire authenticated session, MFA4PD checks the user's GPS location. If any location mismatch occurs, the process to establish a secure session is aborted. Also, in theory, any ongoing session will be terminated immediately for security reasons. This feature might prove useful in case a user leaves the location of a public display without logging out. However, the evaluation of this feature or the accuracy required from GPS data in order for this concept to work in an everyday scenario will be carried out in future work.

For public displays, we limit the number of entered codes per system, location, and time to additionally prevent brute-force attacks. Again, the time-limited one-time-code limits also the possibility of brute-force attacks.

In summary, with regard to security, the system's concept offers protection on the client side against contemporary threats, such as shoulder surfing attacks, thermal attacks, or smudge attacks. Apart from client-side attacks, backend systems as well as the module's communication might also be vulnerable to attacks, which we outline in the next section.

b) Backend security

The users are identified and authenticated by MFA4PD through their credentials, which they enter inside the mobile app. These currently consist of a combination of a username and password. SAM.F validates the credentials. On credentials mismatch, a login is not possible. Additionally, SAM.F checks the mobile device identification number, which is exposed by both Android and iOS system's API. On mismatch to previous devices used, an additional confirmation is required, which we plan to implement via SMS.

The communication between mobile devices, SAM.F and MFA4PD as well as its public display component is SSL-secured and uses token-based API access. Thus, the communication could suffer from all exploit issues that SSL faces, e.g., a man-in-the-middle attack (MiTM). Means to avoid these vulnerabilities concern the underlying systems running SAM.F or MFA4PD, or accessing them, as well as the networks security configuration.

The database used internally by SAM.F is not accessible directly.

In summary, for the current prototype setup, the security measures are sufficient. In future work, we will also address the question of whether the server can be compromised by other means.

V. Validation and Discussion

In this section, we briefly illustrate validation results for this work as well as future work and discuss our approach.

1) Validation Results and Future Work

We tested the prototype under laboratory conditions with mobile devices running Android with Firefox, Edge and Chrome Web browsers. In all tests, we were able to complete the authentication process. However, an evaluation in an everyday setting with a heterogenic group of users is still pending and scheduled for later this year, as outlined below.

In the evaluation we also focus the question, whether users prefer the Web application or the native mobile application.

Although this work does not focus on implementing more factors at this stage, together with the knowledge factor, the system can be extended with *biometrical* factors, using supplementary sources for MFA, such as fingerprint scanners, facial recognition, or voice biometrics. Mobile devices today offer these types of biometrical sensors. However, Web-based access to these sensors is prohibited by the browser's API. The new Xamarin-based mobile application can however access these sensors and we are planning on extending the mobile application's features.

In addition, the system still has to be evaluated quantitatively with a larger number of users, for example with regard to system's performance, usability, and the user's acceptance. The latter might depend on factors such as the setting the system is applied in.

2) Discussion

Public display authentication using the concept outlined in this contribution presents a feasible way, especially with the limitations of our scenario of minimal and no additional hardware requirements, as well as the limited browser capabilities for mobile devices.

Continuing the development with a mobile application that directly runs on smartphones however, new possibilities emerge.

One possibility is to display a QR code on the public display. After scanning the QR code with the mobile application, the session automatically gets authenticated.

Although implementations exist offering QR code readers for Web-based use, overall device compatibility remains an issue. For this reason, in the purely Web-based approach we did not use a Web-based QR code reader and decided to design the one-time-code mechanism.

In the future, we would have to evaluate, whether users prefer the mobile application over the Web application to authenticate themselves on their mobile devices.

The mobile application requires the users to download the app, but with QR-based authentication provides a lighter and faster authentication mechanism. Added biometrical checks using the mobile app could improve security when identifying users.

The Web application is light-weight, does not require a download nor an installation and could be used as so-called captive portal for local (public) Wi-Fi-hotspots deployed in range of public displays.

Both solutions can also co-exist.

For the purpose outlined, with MFA4PD this article presents a feasible solution that does not require additional hardware. The further development enhances the means, by which the MFA for public displays is achieved, as outlined in the next section.

VI. Conclusion

With the Semantic Ambient Media Framework (SAM.F), this contribution presents a framework that semantically interconnects (a) *media*, (b) *devices and applications*, and (c) *services*. The practical scenario illustrated describes the use of SAM.F together with MFA4PD to provide means of a secure method of multi-factor authentication for public displays and means of content retrieval from the semantic repository.

SAM.F provides Web-based access for devices and applications and features a service-based architecture, which allows for interaction with media, such as, e.g., text, pictures, audio, video, 3D objects, or 3D scenes. The concept of SAM.F regards Semantic Media independently of their encoding and automatically transcodes or converts media, where necessary and possible, to meet contexts', applications', and devices' specifications or criteria.

Using SAM.F also solves the problem of media being isolated for use in a single application or on a single device, as SAM.F interconnects users and their devices through its services and Semantic Media.

SAM.F can be used in contexts where interaction with Semantic Media is intended. Through technological means, SAM.F especially supports mobile contexts, e.g., through the application and device-specific provisioning of Semantic Media. Thus, SAM.F offers an enormous potential for exploiting new information sources, e.g., by the relationships of different informational modalities encoded semantically.

In future work, together with our project partner, the *Society for Audiovisual Archive of German-language Literature* based in the Hanseatic City of Bremen, we will utilize SAM.F as technical foundation to digitally enrich a cultural center for German literature. In this research project, SAM.F will interconnect media from various archives or libraries focusing on German literature and make them available on-site using public displays.

At the cultural center, the physical space will be enriched with digital media served provided by SAM.F. Curators will be enabled to adjust the exhibitions contents on-site by using dedicated functions accessible after authenticating on the public displays. User's will be served with personalized digital contents and personalized view after logging in on public displays.

Public display personalization is achieved through means of identifying the visitor (user) using authentication. Authentication on public displays is vulnerable to various attacks and technically presents a challenge, whenever public displays are connected to protected networks that are inaccessible for other devices and public displays are not equipped with dedicated user authentication hardware.

In this contribution, we present a technical solution, which addresses these challenges with a minimal technical solution. This makes use of a multi-factor authentication (MFA) applying the factors of ownership, knowledge and location. Not requiring any hardware upgrades for public displays, the solution implemented as a prototype makes use of the personal mobile devices of users, connecting them, as well as public displays to SAM.F.

Multi-factor authentication for public displays using SAM.F presents a feasible solution to the security issues public display authentication have. The solution presented securely authenticates users and lets them access private, restricted, or personal contents as well as sensitive functionality from and in SAM.F.

We have technically validated our approach under laboratory conditions. In the future, we plan to evaluate the system with a large number of users under everyday conditions. Research questions in this area also relate to the degree of security measures, that users are willing to accept in their everyday dealings with digital systems, as well as the question of how they perceive security issues with regard to their use of personal and private data and contexts on public displays.

It is our hypothesis that providing meaningful digital content in a body- and space related environment fosters mindful knowledge.

The Kingsbridge Research Center is a non-profit research company based in the United Kingdom. With our research it is one of our goals to strengthen the use of digital technology in public environments in our digital society. We achieve this goal through our scientific and project-oriented work. Currently, our non-profit activities and the development of new future-oriented projects is funded privately. At a time, when many are confronting digitization with skepticism and uncertainty, we are committed to communicating security in the mindful use of these technologies and through fostering awareness.

References

[1] D. Bouck-Standen and J. Kipke, 'Multi-Factor Authentication for Public Displays using the Semantic Ambient Media Framework', in *ADVCOMP'19*, *Best Paper Award*, IARIA, Porto, Portugal, 2019, pp. 30-35.

[2] D. Bouck-Standen, 'Introducing SAM.F: The Semantic Ambient Media Framework', in *AMBIENT'19*, IARIA, Porto, Portugal, 2019, pp. 40-45.

[3] A. Whitmore, A. Agarwal, and L. Da Xu, 'The Internet of Things—A survey of topics and trends', Inf. Syst. Front., vol. 17, no. 2, pp. 261–274, Apr. 2015.

[4] Eurostat, 'Internet use by individuals', 260/2016, Dec. 2016.

[5] S. Vrochidis, B. Huet, E. Y. Chang, and I. Kompatsiaris, Big Data Analytics for Large-Scale Multimedia Search. John Wiley & Sons Ltd, 2019.

[6] C. Vassilakis et al., 'Interconnecting Objects, Visitors, Sites and (Hi)Stories Across Cultural and Historical Concepts: The CrossCult Project', in Digital Heritage. Progress in Cultural Heritage: Documentation, Preservation, and Protection, Cham, 2016, pp. 501–510.

[7] E. Williams and J. Yerby, 'Google and Facebook Data Retention and Location Tracking through Forensic CloudAnalysis'. SAIS 2019 Proceedings. 3, electronic version.

[8] T. Kubitza, S. Clinch, N. Davies, and M. Langheinrich, 'Using Mobile Devices to Personalize Pervasive Displays', SIGMOBILE Mob Comput Commun Rev, vol. 16, no. 4, pp. 26-27, Feb. 2013.

[9] A. Ometov et al., ‘Multi-Factor Authentication: A Survey’, Cryptography, vol. 2, pp. 1-31, 2018.

[10] M. Eiband, M. Khamis, E. von Zezschwitz, H. Hussmann, and F. Alt, ‘Understanding Shoulder Surfing in the Wild: Stories from Users and Observers’, in Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems, New York, NY, USA, 2017, pp. 4254-4265.

[11] Y. Abdelrahman, M. Khamis, S. Schneegass, and F. Alt, ‘Stay Cool! Understanding Thermal Attacks on Mobile-based User Authentication’, in Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems, New York, NY, USA, 2017, pp. 3751-3763.

[12] K. Mowery, S. Meiklejohn, and S. Savage, ‘Heat of the Moment: Characterizing the Efficacy of Thermal Camera-based Attacks’, in Proceedings of the 5th USENIX Conference on Offensive Technologies, Berkeley, CA, USA, pp. 6-6, 2011.

[13] E. von Zezschwitz, A. Koslow, A. De Luca, and H. Hussmann, ‘Making Graphic-based Authentication Secure Against Smudge Attacks’, in Proceedings of the 2013 International Conference on Intelligent User Interfaces, New York, NY, USA, 2013, pp. 277-286.

[14] M. Khamis, R. Hasholzner, A. Bulling, and F. Alt, ‘GTmoPass: Two-factor Authentication on Public Displays Using Gaze-touch Passwords and Personal Mobile Devices’, in Proceedings of the 6th ACM International Symposium on Pervasive Displays, New York, NY, USA, 2017, pp. 8:1-8:9.

[15] DESTATIS, ‘Average internet use by individuals’, Survey on the private use of information and communication technologies (ICT), Online: https://www.destatis.de/EN/Themes/Society-Environment/Income-Consumption-Living-Conditions/Use-Information-Technologies/Tables/use-internet-age-ikt.html, Sep. 2019.

[16] T. Berners-Lee, ‘The Semantic Web’, Sci. Am., pp. 30–37, 2001.

[17] F. Nack, ‘The future in digital media computing is meta’, IEEE Multimed., vol. 11, no. 2, pp. 10–13, 2004.

[18] L. F. Sikos, ‘RDF-powered semantic video annotation tools with concept mapping to Linked Data for next-generation video indexing: a comprehensive review’, Multimed. Tools Appl., vol. 76, no. 12, pp. 14437–14460, Jun. 2017.

[19] C. Bizer, T. Heath, and T. Berners-Lee, ‘Linked data - the story so far’, Int J Semantic Web Inf Syst, vol. 5, no. 3, pp. 1–22, 2009.

[20] D. Bouck-Standen, ‘Construction of an API connecting the Network Environment for Multimedia Objects with Ambient Learning Spaces’, Master Thesis, DOI: 10.13140/RG.2.2.12155.00804, University of Luebeck, Luebeck, Germany, 2016.

[21] K. Blumenstein et al., ‘Bringing Your Own Device into Multi-device Ecologies: A Technical Concept’, in Proceedings of the 2017 ACM International Conference on Interactive Surfaces and Spaces, New York, NY, USA, 2017, pp. 306–311.

[22] P. J. Denning, Ed., The Invisible Future: The Seamless Integration of Technology into Everyday Life. New York, NY, USA: McGraw-Hill, Inc., 2002.

[23] U. Yadav, G. S. Narula, N. Duhan, and B. K. Murthy, ‘An overview of social semantic web framework’, in 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), 2016, pp. 769–773.

[24] C. Wang, H. Yang, and C. Meinel, ‘A deep semantic framework for multimodal representation learning’, Multimed. Tools Appl., vol. 75, no. 15, pp. 9255–9276, Aug. 2016.

[25] P. A. Shaw, M. A. Mikusz, P. T. Nurmi, and N. A. J. Davies, ‘Tacita-A Privacy Preserving Public Display Personalisation Service’, UbiComp 2018, pp. 448-451, 2018.

[26] N. Memarovic, I. Elhart, A. Michelotti, E. Rubegni, and M. Langheinrich, ‘Social Networked Displays: Integrating Networked Public Displays with Social Media’, in Proceedings of the 2013 ACM Conference on Pervasive and Ubiquitous Computing Adjunct Publication, New York, NY, USA, 2013, pp. 55-58.

[27] M. Mannan and P. C. van Oorschot, ‘Using a Personal Device to Strengthen Password Authentication from an Untrusted Computer’, in Financial Cryptography and Data Security, Berlin, Heidelberg, 2007, pp. 88-103.

[28] P. Oliveira and P. Gomes, ‘Instance-based Probabilistic Reasoning in the Semantic Web’, in Proceedings of the 18th International Conference on World Wide Web, New York, NY, USA, 2009, pp. 1067–1068.

[29] C. Tzelepis et al., ‘Event-based media processing and analysis: A survey of the literature’, Image Vis. Comput., vol. 53, pp. 3–19, 2016.