FRI-ONLINE-1-CCT1-14

APPLICATION OF SMART CARDS IN PERSONALIZED EDUCATION SOFTWARE AND ATTENDANCE TRACKING

Assist. Prof. Pavel Zlatarov, MSc
Department of Computing,
"Angel Kanchev" University of Ruse
Tel.: 082 888 855
E-mail: pzlatarov@uni-ruse.bg

Assoc. Prof. Galina Ivanova, PhD
Department of Computing,
"Angel Kanchev" University of Ruse
Phone: 082 888 855
E-mail: giivanova@uni-ruse.bg

Abstract: *The paper explores possible uses of smart cards in the context of a modular, personalized learning system. Personalized learning has been steadily increasing in demand, especially during the last few years' events and the shift towards online learning in all levels and stages of education. It entails flexibility and adaptivity of the learning system and content to each individual learner's needs. As a consequence, personalized learning systems require reliable authentication methods to successfully identify the learner and tailor the learning experience accordingly. Smart cards and public key cryptography have been widely adopted for a lot of uses, such as access control, payment applications, digital document signing, used as identity documents and as an alternative or in addition to traditional authentication methods (e.g., password-based authentication). The paper discusses their use as a quicker, simpler, and more interactive method of authentication, collection and storage of relevant data, and subsequent personalization of learning systems. Possible architectural designs, several implementation variants and a proof of concept are also introduced.*

Keywords: *Personalized learning, smart card, authentication, interactivity*

INTRODUCTION

Technology has played an increasingly vital role in all stages of education, allowing for the development of numerous novel approaches in delivering educational content and services. In the light of the recent events of the past couple of years and the world pandemic conditions, demand for modern technological solutions and innovative educational approaches has surged more than ever, especially with the increasing transition to distance and online-based learning.

One of the educational approaches that is highly technology-driven is personalized learning, which is based on personalizing the educational approach and content based on various individual properties of the learners, including (but not limited to) their level of development, strengths, and weaker points and whether they have special needs or not, etc. Personalized learning strives to replace or augment more traditional methods, where the educational process and content are identical for most or all learners. The emergence of personalized education has led to multiple technology solutions being development for the purpose.

Since personalized education relies heavily on determining the individual needs of the learner, such systems would require methods for fast and accurate identification and authentication of each learner to grant them access to relevant content. While there are some traditional identification methods (e.g., username and password-based authentication) that could be used, they are not applicable in all cases or all educational environments.

This paper discusses and explores the usage of smart cards as a quick, simple, reliable, and interactive method to authenticate learners and store relevant data. Smart cards are widely available, widespread, and already used in many industrial and consumer applications, while also

being inexpensive and relatively easy to use. Architectural designs, implementation variants and a proof of concept are also introduced.

EXPOSITION

Background

Personalized education environments can help educators move away from the traditional methods, where standardized content and education/testing methods are used; while these methods might work fine for some students, certain groups have been shown to exhibit worse information retention, lack of attention and interest, lower overall grades, and a higher tendency of information overload. This was the reason for the emergence of innovative personalized learning methods and systems, which emphasize on the individual approach. They allow the entire educational process, along with its appropriate content (text, images, audio/video, tasks and assignments, curriculum sequences, etc.), to be adapted to the learner's individual needs. The process towards personalization has been made easier with the increasing transition to e-learning systems, especially due to the recent pandemic conditions.

To achieve a high degree of personalization, personalized learning systems need to store an individual profile for each user/learner. Profiles may or may not include identifying information, such as name, age, school grade, etc.; however, in most cases, they are required to store information on the learner's level of development and special needs (if any), previous grades and results, and log some high-level actions of the learner. This way, a personalized learning system can base further personalization and recommendations of learning content on known details and previous experience of the learner, and achieve a much higher degree of personalization, while also allowing educators to retain full control of the process.

Since the profile is the base of a personalized learning system, it will also need a secure and reliable way to authenticate and authorize learners in order to make use of the full potential of the system. When it comes to authenticating users, there are a lot of options, with varying degree of security and ease of use. Some of these can include:

- **Username and password-based authentication**, where users need to enter a username (or email address) and a password to access the system. While this method is reasonably secure (provided that it is implemented correctly and a sufficiently strong password is used), it can be inconvenient for certain user groups and classroom settings, such as younger users or users with special needs.
- **PIN-based authentication**, where users are required to enter a numeric code of varying length (usually 4 to 8 digits). This is similar to the username and password method, and may require selecting the appropriate user profile beforehand by another means (e.g. by entering an identifier or choosing from a grid of profile pictures).
- **Barcode-based authentication** – each user is given a unique printed barcode, such as a traditional one-dimensional barcode (similar to those used in item tracking) or a two-dimensional code (such as a QR code), that they may scan using specialized hardware or a smartphone application to authenticate. It can pose some serious security issues, as the code can be copied by different means. (Gagare, P. S., Sathe, P. A., Pawaskar, V. T., & Bhave, S. S., 2014)
- **Mobile authentication** using text messages, or a smartphone app. Requires the user to have a mobile device to authenticate.
- **Smart card authentication** – requires the user to insert or tap a smart card or a similar token to a connected reader device.

While most of these authentication methods have been used in various e-learning systems, the focus of this paper is smart card authentication, as this method provides reasonable security (if implemented correctly) and can also be used to add an interactive element to the user authentication experience. Furthermore, in the classroom setting, it can not only serve as a method to access e-learning systems, but to also track class attendance quickly and efficiently, as

traditional, non-electronic attendance tracking methods have been proven to be less efficient and prone to errors (Bejo, A., Winata, R., & Kusumawardani, S. S., 2018).

Smart cards and their applications

Smart cards usually take the form of a plastic card with some form of an integrated circuit embedded inside the plastic. While plastic cards are the most common form factor, other form factors (such as keychains, tokens, charms, and bracelets) have been known to be in widespread use. A few of the smart card form factors are shown on Fig. 1.

Fig. 1 Examples of smart card form factors and a card reader

To make use of the integrated circuit's capabilities and to interact with the smart card, a card reader (Fig. 1, bottom right) needs to be used. Card readers are designed to communicate with the integrated circuit using the smart card's interface and can either be standalone or connected to a general-purpose computer system.

Generally, modern smart cards support one of two interfaces:

- **Contact** – the card has exposed electrical contacts, which make direct electrical contact with corresponding contact points in the card reader. From there, direct electrical signals are used to provide power to the integrated circuit and communicate with it.
- **Contactless** – the integrated circuit is powered and communicates with the reader wirelessly, using radio frequency identification (RFID). To be read successfully, a smart card needs to be held a few centimeters near the card reader, and no direct contact between the two is necessary.

Smart card integrated circuits can be divided into a few categories, some of which are:

- **Memory smart cards** can store a certain amount of data, which can be read using a standard smart card reader and compatible software. The memory can optionally be encrypted with various encryption protocols to achieve a higher degree of security.
- **Microprocessor smart cards** contain a low power chip that shares a lot of components with a standard computer system, such as a microprocessor, memory, input/output devices and an operating system. These smart cards can be programmed using certain standard programming languages and frameworks, and thus can serve for various purposes. Modern microprocessor cards can even contain multiple applications and act as a different card, depending on the circumstances and the system they are interacting with.

- **Cryptographic smart cards and secure access modules** are a variation of the microprocessor smart cards that contain hardware dedicated to cryptographic operations, making them suitable for electronic identity and security applications.

Due to their versatility, smart cards have numerous applications in all aspects of everyday life, including (but not limited to) electronic payments and banking, telecommunications, e-identity and administrative services, access control, and digital signing, among others. Since smart cards are flexible, new applications can easily be developed as well. Their flexibility, versatility, reliability, and relatively low cost makes them a reasonable candidate for use in personalized learning, as they don't require remembering credentials or have a steep learning curve to use. Furthermore, smart integrated circuits can be integrated into various objects, such as bracelets, tokens or toys, which opens possibilities for adding interactive or game-based elements to e-learning or personalized learning systems.

A lot of smart card applications require cards to be used as devices for secure storage of cryptographic keys and certificates, namely electronic identity and document signing. In this context, the X.509 standard, which defines terms such as certificate and certification authority, and a specific structure for the certificates (the main component of which is a public key), can be used. Smart cards are among the most used certificate storage devices, as they can provide high enough security for key generation and storage.

Proposed solution and architecture

Considering the advantages of smart cards, a system used to authenticate and track attendance of various types of learners has been developed. The architecture of the proposed smart card-based solution is shown on Fig. 2.

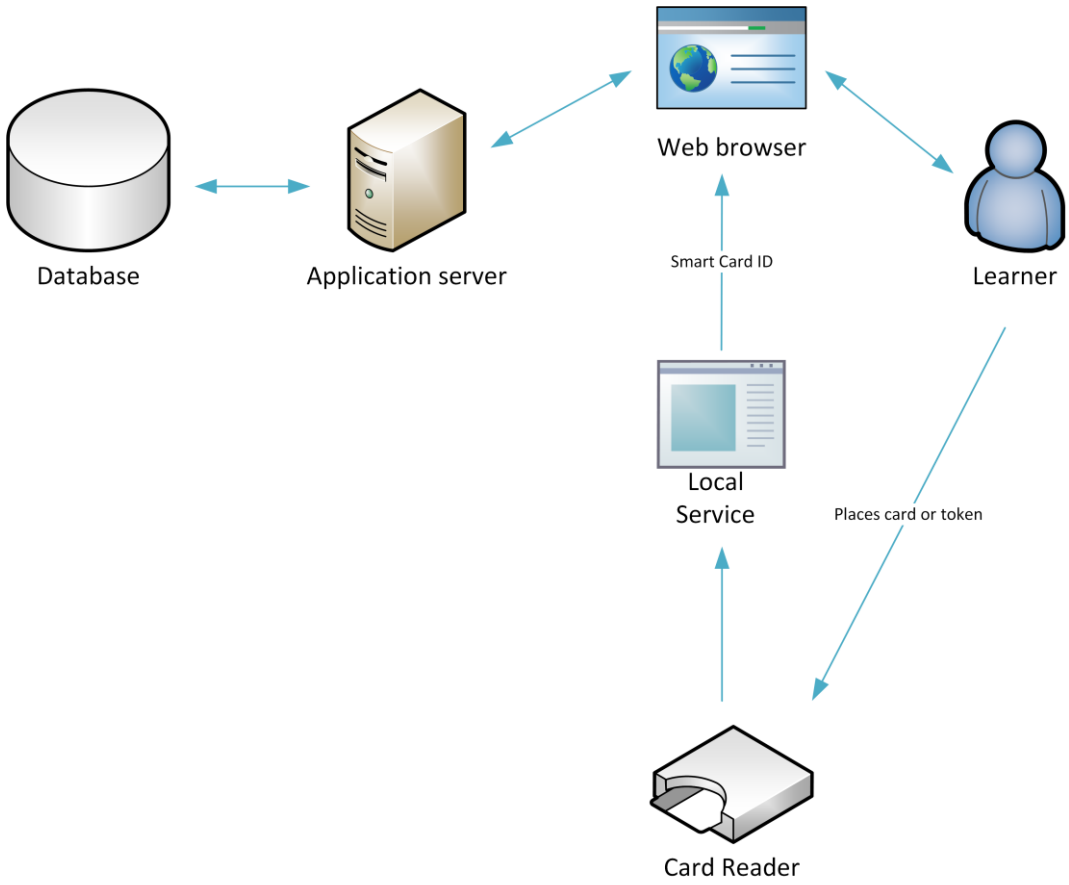

Fig. 2 Proposed solution architecture

The solution builds on the fact that each smart card has a unique identifier, which can be used to distinguish each individual smart card (and thus learners) with high enough certainty and reliability. The following modules can be distinguished:

- **Web browser**, which runs on the learner's computer or mobile device and provides the user interface for the system. It also communicates with the local service module (if available) via WebSocket.
- **Local service**, responsible for communicating with the smart card via a smart card reader. This module is needed since web browsers, in their default configuration, cannot communicate with smart card APIs provided by the operating system. The local service module exposes a WebSocket endpoint, which is used by the user interface to determine if the service is installed, and smart card authentication can be used. If so, the module will send the relevant smart card identifier to the user interface module as soon as a compatible smart card is inserted into or presented against the card reader.
- **Application server**, which provides the application logic and checks identifiers against a database. Once the identifier is verified, access is granted to the learner, and their presence logged, if desired.
- **Database**, responsible for storing the smart card identifiers and other data relevant for the system.

The user interface for an implementation of the proposed architecture, showing a login screen and the monitoring interface for the local service, is shown on Fig. 3 and Fig. 4.

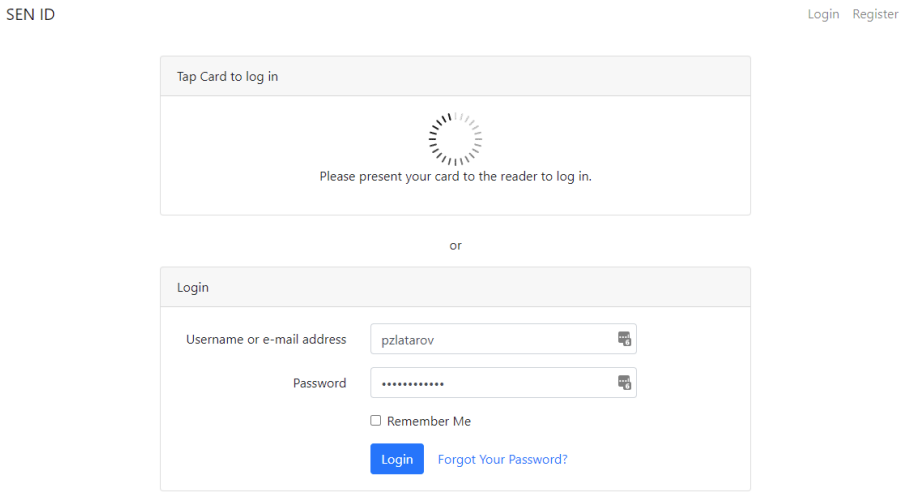

Fig. 3 Smart card login screen

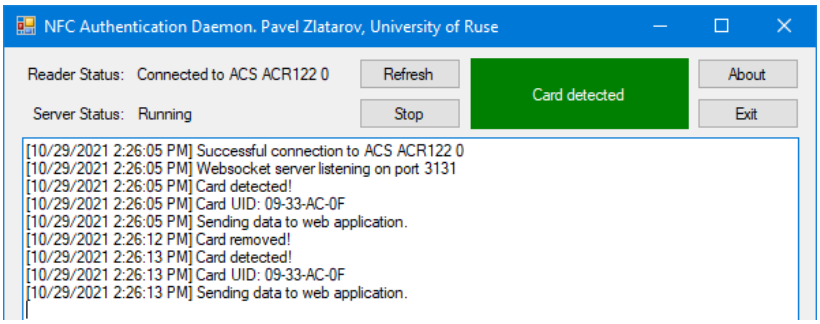

Fig. 4 Local service monitoring interface

The main advantages of the proposed solution are that it is easy to implement and does not require any additional infrastructure, beyond what is already required for an e-learning system, and the installation of the appropriate card readers and software on the devices that will be used by learners. Furthermore, it is cost effective, as it relies on smart card identifiers, meaning that any existing standard smart cards (such as transport passes, loyalty cards, etc.) can be used if desired, and the smart card's content and purpose does not need to be modified. However, this poses some security concerns, as smart card identifiers are generally hard to reproduce (unlike visual means, such as barcodes), but not impossible. To address this, an alternative has been developed, as shown on Fig. 5. The overall system architecture is largely unchanged; however, instead of relying on a local service that reads smart card identifiers, the web application directly requests a client certificate to be provided. Since client certificates can be stored on smartcards and are also supported by most major browsers, the local service is not needed. However, implementing this solution requires the use of at least two certificate authority servers, which will handle the certificate issuance and management. The root certificate authority should be kept offline unless needed, as it could be used to create other intermediate certificate authorities, thus compromising security.

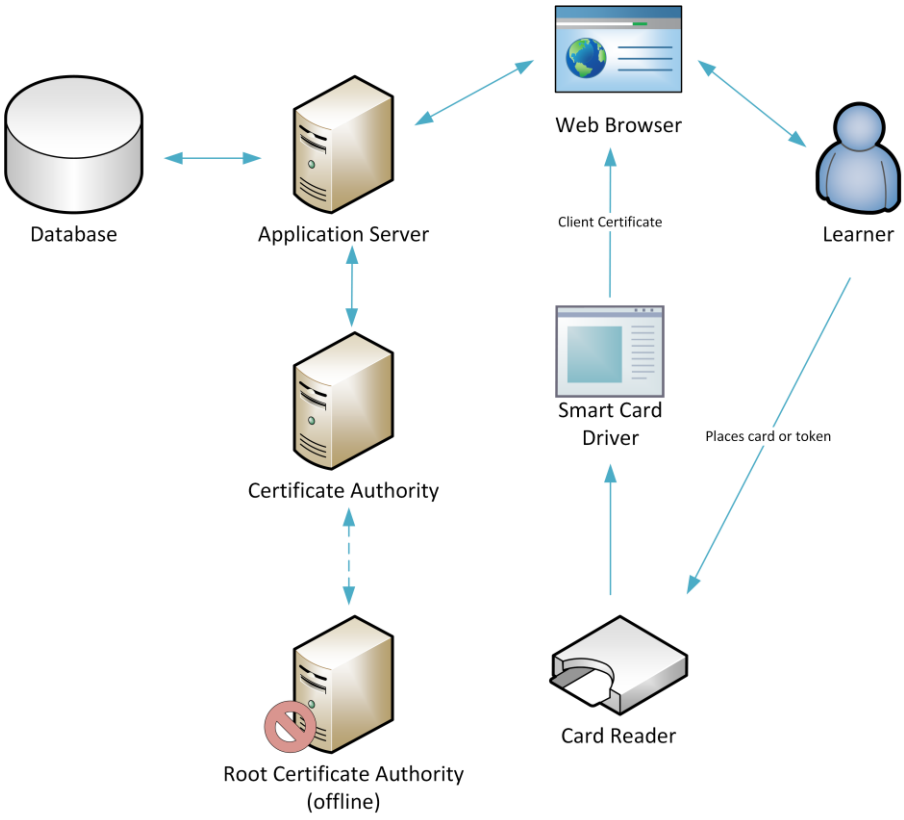

Fig. 5 Alternative solution architecture

The proposed alternative solution provides a better degree of security; however, to store certificates, the implementation needs to make use of either microprocessor cards or cryptographic cards, which might be less cost effective and may introduce a considerable administration overhead, since a certificate would need to be generated for each user and installed on the smart card before it can be used.

CONCLUSION

Thanks to their versatility and relative ease of use, smart cards have the potential to be a secure, reliable, and effective method for authentication and subsequent personalization of content in a personalized learning system. The solution shown is under deployment and its installation in a classroom setting and active usage with certain groups of learners is underway.

ACKNOWLEDGEMENTS

The paper presents results of work related to project No 2021 – RU – 01 „Design and Construction of a Smart Teaching and Research Laboratory for Doctoral Students - Phase 2“, financed by the Science Fund of the University of Ruse.

REFERENCES

Chen, C. M. (2008). Intelligent web-based learning system with personalized learning path guidance. Computers & Education, 51(2), 787-814.

Gagare, P. S., Sathe, P. A., Pawaskar, V. T., & Bhave, S. S. (2014). Smart attendance system. International Journal on Recent and Innovation Trends in Computing and Communication, 2(1), 124-127.

Bejo, A., Winata, R., & Kusumawardani, S. S. (2018, October). Prototyping of Class-Attendance System Using Mifare 1K Smart Card and Raspberry Pi 3. In 2018 International Symposium on Electronics and Smart Devices (ISESD) (pp. 1-5). IEEE.

Lee, C. H. M., Cheng, Y. W., & Depickere, A. (2003). Comparing smart card adoption in Singapore and Australian universities. International Journal of Human-Computer Studies, 58(3), 307-325.

Rosli, K., & Ahmi, A. (2011). Awareness and adoption of university smart card: The case of UUM. Journal for the Advancement of Science & Arts (IJASA), 2(1), 40-55.

Zlatarov, P., Ivanova, E., Ivanova, G., & Doncheva, J. (2021). Design and Development of a Web-based Student Screening Module as Part of a Personalized Learning System.