Towards a Model of Client-Driven Access to Public e-Services

József Károly Kiss(✉), Peter József Kiss, and Gábor Klimkó

MTA IT Foundation, Budapest, Hungary
mtaita@t-online.hu

Abstract. The take-up of the usage of public e-services in Hungary is slow, though a lot of efforts were exerted in order to accelerate the process. The paper points out barriers rooted in the traditional logic of access to public e-services in which clients are required to use the same e-authentication technique and way of electronic document exchange. We present a client-driven model that gives the freedom of choice to the client with respect to the e-authentication technique as well as the document exchange to be used, thereby eliminating these barriers. A simplified form of the model was enacted by the law and is now being implemented in Hungary.

Keywords: e-government enterprise architectures · Electronic identity · Identity management · Electronic document exchange

1 Introduction

In order to enable usage of electronic government services (public e-services for short) in Hungary, a single and unified electronic authentication method and contact channel called "Client Gate" was introduced in 2005 [1]. Under the "Client Gate" brand the Hungarian state offers a free electronic authentication service that uses username/password pairs. Citizens are required to register for the "Client Gate" service in person. The service includes the registration of one e-mail address of a client as well as a limited but free storage capacity where clients can upload and download their electronic documents to be used during exchanges of documents with public authorities. Uploaded documents are certified by digital time stamps; all files are handled via the Government Portal https://magyarorszag.hu/. Later certain public administration organisations also got their own similar electronic service, called the "Office Gate". The Office Gate uses username/password authentication, too [2].

Though politicians envisioned a widespread usage of the Client Gate, at the beginning there was a low level of interest in using it [3]. Having experienced this situation, the Hungarian Government made the usage of "Client Gate" services compulsory for certain taxation-related activities in a wide circle of enterprises and entrepreneurs. Consequently the number of registered "Client Gate" users increased steadily and significantly.

© Springer International Publishing Switzerland 2015
A. Kő and E. Francesconi (Eds.): EGOVIS 2015, LNCS 9265, pp. 117–131, 2015.
DOI: 10.1007/978-3-319-22389-6_9

There are more than 1.86 million registered Client Gate users today, but the seemingly continuous development is mainly due to the fact that the usage of the Client Gate service became mandatory by law for a new group of users from time to time.

At the end of 2013 there were 718,792 companies, 380,794 individual entrepreneurs and 684,064 private individuals (with tax number) performing independent activities, that is, all together 1,783,650 taxpayers with tax numbers. Those who have a tax number are obliged to use Client Gate services. However, there are 3.6 million employees among Hungarian taxpayers, who are not obliged by law to use Client Gate services [4]. It is now clear that this group does not use Client Gate services heavily; that is, it is not within their obvious natural needs.

We do not know exactly what percentage of the registered Client Gate users conduct personal (i.e., for his/her own purposes) electronic business with the government. In order to estimate this data, let us consider the number of visitors to the Hungarian Government Portal, https://magyarorszag.hu/.

The number of visitors is usually in the range of 450.000-500.000 per month. If we consider the 5.4 million Hungarian taxpayers (this figure does not include students and pensioners), the current rate of e-government service users is at most 20 % of the potential beneficiaries.

The primary driver of using e-government services is their availability, but in our case it is not a real issue. Although in principle, everybody of the 5.4 million Hungarian tax-paying population could use the electronic tax form service in 2013 there were 2.4 million personal client contacts in the tax customer offices [4].

One may assume that potential users are afraid of using electronic services in general. In contrast, however, when the Hungarian Tax Office offered a comfortable remote (phone) service, the number of users showed a very dynamic increase. When employment relationship between private persons for the performance of housework was introduced, employers were let to notify the Tax Office by phone as well as through the Client Gate. Almost 64 % of the employers chose the phone and only 36 % used the Client Gate [4].

As Internet penetration in Hungary is high enough there must be other barriers that block the usage of e-services. The relatively low usage of e-government services might not be attributed to a limited service portfolio, either [5]. This statement was confirmed in the e-Government Benchmark Report in 2014, where the recommended action for Hungary was to invest to enable more people to actually use services [6]. We believe though that if we understand and serve the real needs of citizens better, a higher usage rate could be achieved. This is the reason why we looked for a more attractive model of accessing electronic public services.

2 Goal and Method of the Study

The starting point of our study is that there are a reasonable number of clients who posses Client Gate access and there are also working public e-services in

Hungary that are useful and valuable for the clients, but still take-up of public e-services is relatively low.

We wanted first to identify certain barriers that hinder the widespread usage of public e-services. We looked for possible usability, privacy and security concerns that could be removed by organisational and technical solutions. Usability and privacy/security are in correlation; the higher the privacy/security level of an e-service, the more uncomfortable is its usage. We did not study human (psychological and sociological) aspects as we were not interested in studying the whole population but only those who are digitally literate. (Note that 'digitally literate' does not equal to being an information technology professional.) We are talking about such potential clients of whom a lot have Internet access anyway. As Client Gate services are free in the sense that clients do not have to pay for them, therefore the cost of public e-services is not a potential barrier.

In order to understand the real security needs of the citizen we used data acquired during the process of setting up new one-stop-shop customer service centers called "Government Windows" in Hungary [7]. Citizens will be able to conduct about 2,300 different types of public administration cases in a Government Window in the near future. These facilities are introduced as part of the structural reform of the Hungarian public administration [8]. We interviewed some officers who participate and direct the reform.

Having identified three barriers we propose a new model that is based on the principle that the client and not the authority should be allowed to choose from separate e-authentication techniques and document exchange methods during the course of doing business with public authorities. The model is based on certain registers and systems; their role will be described in separate subsections. Communication among these systems will be presented with sequence diagrams.

A simplified version of the model was already enacted in Hungarian law and is now being implemented. For the sake of brevity we shall focus on and present the logical model omitting implementation details.

3 Barriers of Widespread Usage of Public e-Services

We are going to point out three barriers that are rooted in the traditional logic in the access to public e-services. Salvodelli at al. gave a comprehensive literature overview on the paradox of the still low adoption of e-government after more than two decades of policy efforts and public investments for the deployment of online public services. They identified 16 different types of barriers among which the lack of digital skills is the most often cited one between 2005 and 2009. The second most important type of barrier is user participation, which is in our focus [9].

When a client uses public e-services there is a need for authentication and often for some form of formal exchange of electronic documents. Issues associated with authentication and the exchange of documents can discourage the usage of e-services. If a client does not intend to use a public e-service in person then s/he should nominate a trustee. Unfortunately, this nomination process also leads to challenges.

Note that it is an evident usability requirement that clients want access to public e-services via devices they are using for other purposes, too. As the use of tablets and smartphones is increasing fast we took this phenomenon as a constraint in our study.

3.1 The Barrier Attributable to a Prearranged e-Authentication Technique

There are a number of electronic authentication techniques available that differ in their strengths. The strength of an electronic authentication technique is usually characterised by the number of applied independent factors (knowledge, ownership, inherence) used as well as the communication channel (Internet, GSM etc.).

In Hungary currently the only form of electronic authentication for public e-services is the Client Gate where citizens use a username/password pair. It is well known that this authentication technique has a relatively low security and this weakness might lead to the limited usage of public e-services.

Austria, Belgium, Estonia and Portugal use smart card technology to support public e-services [10–13]. /Note that there are other European examples, too, see Kubicek's comparative study [14]/. The idea of using such strong two-factor authentication technique seems to be appealing at first glimpse and it was proposed to be used in Hungary, too. Smart card-based electronic authentication, however, was not successful at all in the private sector. For example, in home banking the usage of a bank card that requires a card reader device is practically non-existent in Hungary; other forms of two-factor authentication as one time passwords sent by SMS or tokens are preferred instead.

If we categorise electronic authentication techniques according to whether authentication is done in a controlled environment and with a controlled device or not, the inherent problem of the smart card based e-authentication becomes clear (see Table 1). The typical usage of public e-services happens in an uncontrolled environment with an uncontrolled device. The strength of the same authentication technique in a controlled environment is very different from that of at home (i.e. uncontrolled) environment.

We can conclude that a single e-authentication technique that is purely based on the need of the highest level of security can be a barrier to widespread usage of public e-services.

Table 1. Smart-card based e-authentication situations

e-authentication	With controlled device	With uncontrolled device
In controlled environment (person is present)	e.g. border crossing with biometric passport	e.g. using e-service in an Internet cafe, authentication is done by digital signature
In remote (uncontrolled) environment (person is not present)	e.g. usage of an ATM	e.g. usage of a public e-service from home, or home banking

We found another obstacle attributable to the single, unified e-authentication solution. In Hungary, new one-stop-shop customer service centers called "Government Windows" are to be introduced. In a Government Window clients can conduct about 2,300 different types of public administration cases in the near future.

We classified the 2,300 types according to the security needs of the citizen into three categories. We rank as "high security" needs those cases where the citizen need to provide sensitive, personal data such as health data, social status or penalty data). Cases, where there is no need for sensitive, personal data, were ranked as of low security needs. In these cases the citizen usually notifies or declares something or requests not sensitive data. The remaining cases were ranked as of medium security needs. We found that 74 % of the cases are categorized as low security needs, 11 % as medium and 15 % as high security needs. Therefore it is unnecessary to pose high security requirements on a significant portion of the cases. There are, however, cases where using a low security solution would result in a high risk. One can get the idea that it could be worth linking the required strength (level) of authentication to the type of the case. That is, there should be different authentication techniques available for the citizens. There are countries that have taken steps in this direction (e.g. Estonia, see below). In Hungary, the use of mobile phones for Client Gate authentication is being developed, too.

In this approach the client is allowed to select from the authentication techniques but specific types of cases determine the applicable authentication techniques. This, however, still does not explain why the usage of services based on the username/password authentication technique does not reach a higher proportion for cases with low security needs. The underlying reason is that the Client Gate approach as well as other initiatives in the public administration is based on a simplified understanding of the clients. Clients are viewed as a basically homogenous group, however, that is a wrong perception.

In summary, we identified a significant barrier that inhibits the widespread usage of public e-services. Governments typically offer public e-services with an all or nothing logic; that is, if a citizen gets his/her e-authentication credentials, then all available public e-services are allowed to be accessed with these. The client is not allowed to select among different e-authentication techniques, neither can s/he declare his/her wish that certain types of cases should be treated personally.

3.2 The Barrier Attributable to a Prearranged Way of Electronic Document Exchange

An essential element of conducting e-business with public authorities is the exchange of information. Though there are on-line interactive technical solutions for this purpose, the significance of the exchange of electronic documents has just slightly decreased – if a case ends with a resolution issued by the authority concerned, the client (for his/her own sake) should receive an authentic copy of it. In contrast, in the business sector document exchange is often simply based

on e-mail systems, parties trust in each other. To support the exchange of electronic documents for public e-services in Hungary, a free central storage facility is available for Client Gate owners. This service is available for each Client Gate user and it is always on – if this service fails, that is legal reason for exemption in case of being late.

A mistrustful client, however, may not be happy with this service. Using a central document storage facility means that all electronic documents of the client can be found at a well-defined place. If we compare the consequences of hacking a transactional e-government system and a central storage facility, the differences are striking. The annual number of cases (i.e. documents) at an average Hungarian public authority is about 2 million. That is, on any working day, roughly thousands of documents are processed within a couple of minutes. The defence against hacking today is often done by on-line surveillance, which means that intrusions are detected within (maximum) a couple of hours and the necessary countermeasures are taken. Therefore in case of hacking into a public administration system, we might expect the illegal access to maximum of a few thousand documents that are being processed.

The risks are very different in the case of a central storage facility that provides a large scale service. Due to the necessary large bandwidth to the central storage facility more documents can be captured by a hacker during the same period of time. At a transactional system a hacker can only get documents related to specific public administration cases, whereas at the central storage facility documents of separate cases might be found that may enable the building of personality profiles.

The ordinary citizen is reluctant to conform if the state wants to observe and control his/her activities and a central storage facility might be a proper tool to achieve this. Thus it is understandable that citizens do not willingly use the central storage facility and they prefer e-mail as a communication channel. We identified therefore a second barrier against the widespread usage of public e-services.

Note that the individual needs of the clients might be different, too. A citizen might prefer to share a document on Facebook or send it by e-mail; or can manage it separately form his/her private mails.

3.3 The Barrier Attributable to the Assignment to the Client

We found a third barrier that might be the toughest. When using public e-services, the main focus is usually on the secure and precise authentication (assignment) of the client. In practice this approach is not appropriate when

1. there is no need to present the personal data of the client asking for a service at all;
2. it is not the client him/herself but his/her trustee who is going to do the business.

The current Hungarian legislation handles the first issue – in accordance with the personal data protection rules – by introducing four types of electronic authentication.

The second issue, the case of a trustee who can act on behalf of the client in e-services, however, is not handled in Hungarian law. Currently, a Client Gate owner is legally entitled to use public e-services only on their own behalf. The only exception is the Tax and Customs Office where there is a dedicated, paper-based system in which those Client Gate owners who are entitled to act in cases on behalf of a company can be named [15]. A wide-spread use of such a paper-based solution would result in a confusing situation for the clients as they were expected to follow to whom, for what purpose and what period of time a mandate for being trustee was given.

A certain number of citizens do not use Client Gate as they would prefer to have a trustee to act in their cases. The only way to do this would be to disclose their personal Client Gate credentials to their trustee. There is a need for a proper way of authorising trustees, in other words the hiatus of such a mechanism is a barrier.

4 A Client-Driven Model of Access to Public e-Services

According to the traditional logic of e-government, public authorities specified how to run the office work and which e-authentication techniques are allowed. Having identified the aforementioned three barriers as consequences of the traditional logic, we present a model in which rules (precepts) are to be defined by the client and authorities should adapt to those and not vice versa. This is a breakaway from the traditional approach, the client is not enforced to use any authentication technique claimed to be the superior one (e.g. PKI based approaches [16]).

In this model the clients are allowed to give their precepts for specific types of cases, where they declare that

- with which authorities what type of authentication technique should be used (among the available ones), as well as
- who is allowed to act as their trustee.

For example, if the client declares that s/he is willing to authenticate him-/herself only with username/password in a certain type of case, then the proper authority is not allowed to accept smart card based authentication even if the client happens to have a valid smart card. Note that the Indian Aardhaar Authentication Service is similar to this model in the sense that it allows for using different e-authentication techniques. In the Aardhaar system, however, there is a Central Identities Data Repository that contains all the credentials of a client [17]. In the model to be shown there is no need for such a central repository as Identity assertion Providers (IdPs) can store the client's credentials.

The client can also declare that in certain types of cases s/he wants to act personally (i.e., the use of e-services are excluded) only because of possible abuse (note that in principle this should decrease the number of abuses).

The implementation of this model is based on the Central Register of the Clients Precepts (CRCP) where the precepts are stored. In principle it would be possible to have separate registers for precepts, e.g. by branches of government; however such a requirement has not been raised even in the strict Hungarian data protection environment. The reason for having one central register is that storing the client's precepts separately at different authorities would cause a burden for both for the authorities and for the client. Authorities would have to bear the development costs; clients would have to continuously monitor where and what kind of precepts they made. Having separate registers would also lead to the requirement of some form of federation that would increase complexity, too. The solution is to have a central register of the client's precepts.

Let us note the providers of public e-services with $SP_1 \dots SP_n$ identity assertion providers for these e-services with $IdP_1 \dots IdP_m$ and the Document Exchange Providers for these e-services with $DEP_1 \dots DEP_l$. Note that we shall use the expressions "service provider" and "public authority" interchangeably, that is, "public authority" refers to the authority that is responsible to provide the e-service. Having introduced the concept of CRCP the model of operations shown on Fig. 1. could be envisaged (lines represent flow of data between the nodes).

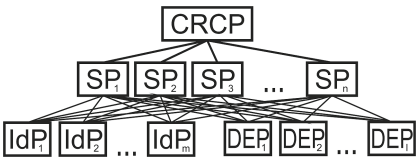

Fig. 1. First-cut architecture of the model

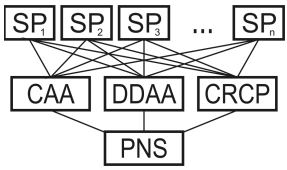

Fig. 2. Architecture of the model

Each service provider is required to use the data stored in the CRCP, that is, precepts for both authentication and document exchange. These precepts specify then which IdP and which DEP should be contacted.

A straightforward implementation of the above model is not appropriate for two reasons:

- each service provider should communicate with each IdP and with each DEP;
- in order to query a client's precepts in the CRCP, a prior authentication of that client should happen, i.e. there would be need for multiple authentications.

These problems can be resolved by using the concept of the 'agent', that is, an intermediary party that manages centrally the flow of data. On that basis we introduce the following agents:

1. The Central Authentication Agent (CAA) offers the services of the available IdPs to the client requesting of an e-service. The e-service providers communicate with the separate IdPs via the CAA.
2. The Document Delivery and Arrival Agent (DDAA) offers the services of the available DEPs to the requesting service provider, and it manages document

exchange between the client and the e-service providers. The DDAA handles incoming and outgoing electronic messages sent by and received from various DEPs. The DDAA also incorporates basic document management functionality; it logs the sending event as well as the event of receiving of a return receipt into the filing register of a service provider.

We introduce one more element in the model, the Periodical Notice Service (PNS). The client's freedom of choice amongst different authentication techniques might lead to the usage of solutions with lower security level. The increase in risk should be compensated with the introduction of some forms of guarantial items. The PNS is such a guarantial item. Electronic events related to a client (e.g. s/he logged in a system, his/her precepts were retrieved from the CRCP; s/he was sent official messages etc.) are to be logged and a summary will be regularly sent to the client by the PNS (if the client asked for it). Thereby the client can check whether somebody cheated him/her and s/he can take the necessary actions (including criminal complaints). The PNS is analogue to the practice of banks that send an immediate SMS notice when somebody logs in the home bank. The PNS, similarly, sends a certified official message that contains the log of related events in a predefined period of time. Note that in order to strengthen confidence in the model other guarantial items might be also needed.

Using CRCP, CAA, DDAA and PNS, the model of operations shown in Fig. 2. can be proposed which is better suited for implementation.

In the next sections we will discuss the functionality of CRCP, CAA, DDAA and PNS in more detail.

4.1 The Central Register of Client's Precepts

The CRCP should contain certified public records. Certified public records should be accepted by the law unless one disputes the content of that record in court in Hungary.

A precept of a client can be generic or specific and it can belong to the following types

- precepts for permitted ways of contact with authorities (personal, by phone, electronic)
- precepts for authentication techniques to be used
- precepts for delivery channels and
- precepts for trustees

A precept can concern a natural person as well as a legal entity. In that way the CRCP manages all variations for nominating trustees. Samples for the possible scenarios are presented in Table 2.

The legal requirements of personal data protection should also be taken into consideration at the implementation of CRCP. In Hungary it is forbidden by law to use a single, universal personal identifier and, as a consequence, the primary key of CRCP that identifies a person should only be known within the CRCP. The CRCP should therefore communicate with other systems with their

Table 2. Scenarios for nominating trustees

	Trustee		
Authorizing entity		Person	Legal entity
	Person	A husband sends his wife to act on behalf of him	A person authorises a law firm to act on behalf of him
	Legal entity	somebody (who is not an official representative) has the mandate to act on behalf of a company	A company authorises an accounting firm to act on behalf of that company

corresponding own primary keys. The CRCP should not store the document containing a precept but only its data content. When a service provider (system) requests a person's precept, the CRCP sends and certifies its data content only. The problem due to the prohibition of using universal personal identifiers can be circumvented by the introduction of the "linking register" (LR). The service based on the LR provides a method of secure interconnection of registers containing personal data. The LR contains encrypted anonymous linking codes that are generated and encrypted separately by the operators of the registers. The detailed discussion of LR is not in the scope of this paper, for our purposes it is enough to know that personal identifiers can be legally obtained.

There should be a service provider for the CRCP, too. A client can enter (store) a precept into the CRCP as the sequence diagram in Fig. 3. shows.

If the public e-service provider SP_1 requests for a certified precept of a person from CRCP, it is provided with the help of the LR as shown in Fig. 4.

Each precept can be specific to a certain type of case and to a certain authority. To enable this feature the CRCP uses taxonomy of concepts as well as that of the authorities concerned.

The CRCP is a critical element from the point of security as the client is allowed to specify low security authentication techniques and communication channels. As a guarantial element the very first so-called "base precept" of a client differs from the other ones. The base precept contains a precept about who and how is allowed to change precepts of the client. The base precept can be created only by a secure way, e.g. personally or such a way where stealing of personality can be excluded. For example, the client can prescribe in the base precept that his/her precepts can only be modified with personal appearance; or s/he can allow it remotely, using a secure authentication technique. The client is also allowed to use precepts for communication via phone. For example, having been authenticated via phone, s/he might give a precept for a trustee.

4.2 The Central Authentication Agent

The task of the CAA is to hide away the complexity of using several IdPs for the systems requesting a client's authentication. The CAA should use a common communication protocol with its requesting parties (service providers), e.g.

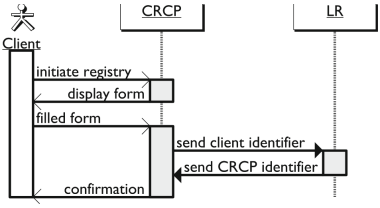

Fig. 3. Entering a precept in the CRCP

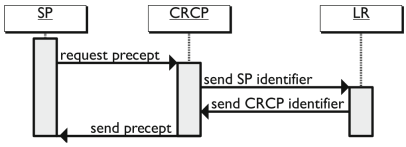

Fig. 4. Retrieving a precept from the CRCP

Security Assertion Markup Language (SAML) that is widely used in EU countries [18]. The CAA, however, might use other protocols in communicating with the IdPs.

The CAA offers the client different authentication possibilities, and, on the basis of the client's choice, it passes the control to the selected IdP. The main steps in the (basic) authentication process are shown in Fig. 5. (note that for the sake of simplicity error handling is not included).

The CAA might offer third party IdPs, too. Third party IdPs sometimes verify such credentials that are not suitable for authentication of the client in the public sector. Google, for example, can verify an e-mail address and this data is not enough to conduct business with the public administration. The CRCP solves this problem as the client is able to specify a third party IdP as well as its credential holder, this data then authenticates him for public e-services. If the client wishes to use a third party IdP, then the CAA can match the acquired data with a query from the CRCP to establish whether there is a corresponding precept. The simplified process is shown in Fig. 6. (from the point when the IdP sends the result to the CAA).

4.3 The Document Delivery and Arrival Agent

It is advantageous to give the user of the public e-services the freedom of choice among contact channels, too. In Hungary the following electronic communication channels are available for document exchange in general:

- storage provided for the owners of a Client Gate
- the secure electronic mail service operated by the Hungarian Post
- e-mail (provided by an arbitrary service provider)
- the official conversion service between paper based document and its authentic electronic document version; including conversion from paper to electronic document and the other way round.

Note that fax services might be still in use in exceptional cases; this can also be integrated in the model if it is necessary. If an e-service allows for using SMS based communication, this can also be managed.

The rationale behind having the DDAA is that the Hungarian public administration still heavily relies on using documents; therefore document management has a distinctive role. Delivery and dispense/distribution of documents (especially with structured data) can be automated with the DDAA services. The

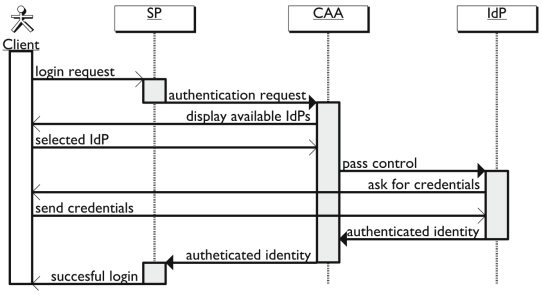

Fig. 5. Authentication via the CAA

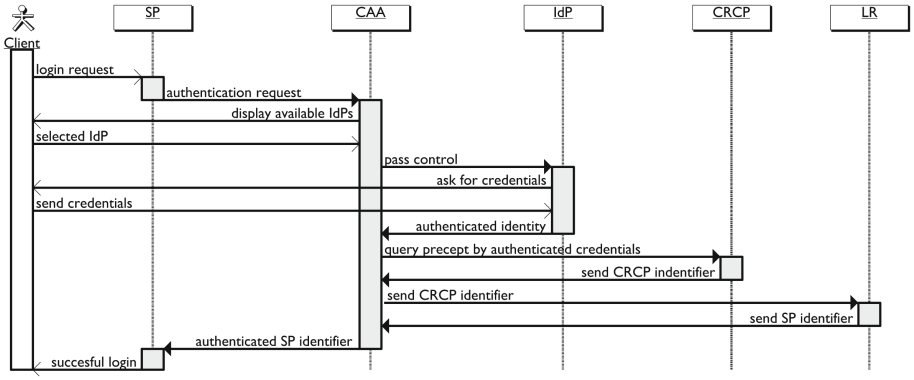

Fig. 6. Authentication by third-party IdP via the CAA

DDAA is able to receive documents sent by the client via different communication channels. According to the precepts of the addressed public authority, the DDAA can virus check and register the arrival of the sent document and upon request of the client, it can create and return a receipt note. The DDAA converts the officially certified (signed) document into the format expected by the selected communication channel; then it sends for delivery and records the delivery event into the filing register of the issuing authority (that is, the authority of which electronic system passes to the document to the DDAA).

The DDAA provides for the return receipt, and it can also check if the return receipt was sent in time and if not, it notifies the sending party (system) of the document. The main steps of this process are shown in Fig. 7. (without error processing).

4.4 The Periodical Notice Service

The client's freedom of choice allows solutions with lower level security to be used but the overall security should not be compromised. This need justifies the introduction of the PNS.

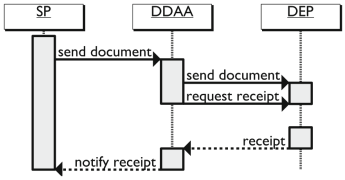

Fig. 7. Document exchange via the DDAA

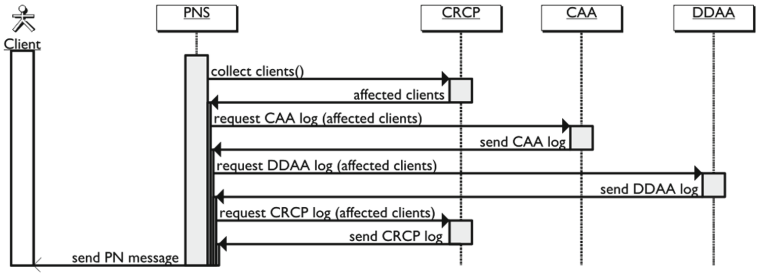

Fig. 8. Processing logic of the PNS

Generally, the necessary level of security can be achieved by two approaches. According to the current prevailing approach the possibility of any abuse should be – in principle – completely excluded. The effectiveness of this approach, however, is questionable. One constraint is the available authentication technique. Security can be comprehended only for the whole system which includes the client; and it is often the client who the weakest point is – for example, he writes his password on a paper and puts it into his drawer.

The other approach to achieve the necessary level of security is to provide feedback to the affected parties; a number of systems work that way. Similarly, the PNS provides feedback to the user of public e-services. It assembles periodical reports containing logs of events for the client that concern him – if he asked for it – over a certain period of time. Such an event may be when the client was authenticated (CAA has the data); a document was sent to him or he sent a document to public authorities (DDAA has the data); or his precepts were used (CRCP has the data). The report assembled by the PNS is typically a digitally signed (certified) document. The main steps of the PNS process are shown in Fig. 8.

The PNS queries in blocks from the LR on a daily basis, and then it batches reports from other registers on the basis of the blocks. The order of the answers is random; this part is asynchronous. On the basis of the batch report the PNS assembles individual reports and it sends them to the clients.

In summary, whatever authentication and communication method the client uses during accessing public e-services, he could detect abuses on the basis of the reports sent by the PNS and therefore he can act upon them. Resolutions of public authorities can be legally challenged; previous status can be restored; in case of personality theft, criminal proceedings can be initiated.

5 Conclusion

In Hungary there are a number of citizens who have the necessary infrastructure to use public e-services but still do not use public e-services extensively. A possible reason for this phenomenon is that the individual comfort and security requirements of the clients have not been taken into consideration in a proper way. We have identified three barriers that are rooted in the simplified picture of the clients which led to an imposed way of e-authentication and document exchange.

We showed a model of client-driven access to public e-services. In this model the client is entitled to decide what kind of communication channel and authentication technique is to be accepted by which authorities; he can decide in which type of case and who is allowed to act on his behalf. The client might also declare that he is not willing to use e-services in certain types of cases. The CRCP, the CAA, the CDAA, the PNS and the LR are the building blocks of the implementation of the proposed model.

A simplified form of the model was enacted by Act CXL of 2004 on the General Rules of Administrative Proceedings and Services and by Government Decree 83/2012.(IV.21) on the regulated electronic administration services and services to be provided by the state. The model is now being implemented in Hungary. The project that built the CRCP and CAA was finished at the beginning of 2015 (Generic Client Authentication Project, EKOP-2.3.8-2012-2012-0001).

References

1. European Commission, eGovernment in Hungary, Edition 16.0. https://joinup.ec.europa.eu/elibrary/factsheet/egovernment-hungary-april-2014-v160 (2014)
2. OECD e-Government Studies: Hungary 2007, OECD Publishing, Paris (2007). doi:10.1787/9789264030527-en
3. Harindranath, G.: ICT in a transition economy: the case of hungary. J. Global Inf. Technol. Manag. **11**(4), 33–55 (2008). http://dx.doi.org/10.1080/1097198X.2008.10856478
4. Nemzeti Adó- és Vámhatóság. 2013 Yearbook of the National Tax and Customs Administration (in Hungarian) (2013). http://www.nav.gov.hu/nav/kiadvanyok/nav_vilaga
5. Csüllög, K., Varga, A.: A survey on mass perception of e-government services in Hungary, Information Society (1/2007) (2007)
6. Directorate General for Communications Networks, Content and Technology Delivering on the European Advantage? eGovernment Benchmark. Final Insight Report: May 2014 (2014). ISBN 978-92-79-38051-8
7. Hajnal, G., Kovács, E.: Government Windows: One Stop Shops For Administrative Services In Hungary (2014). http://www.cocops.eu/wp-content/uploads/2013/10/Hungary-CGov-Government-Windows.pdf
8. OECD, Public Governance Reviews. Hungary: Towards a Strategic State Approach (2015). http://www.oecd.org/publications/hungary-towards-a-strategic-state-approach-9789264213555-en.htm

9. Salvodelli, A., et al.: Understanding the e-government paradox: Learning from literature and practice on barriers to adoption. Gov. Inf. Q. **31**, 63–71 (2014)
10. Aichholzer, G., Strauss, S.: Electronic identity management in e-Government 2.0: Exploring a system innovation exemplified by Austria. Inf. Polity **15**(1–2), 139–152 (2010)
11. Marin, I., Audenhove, L.: The Belgian e-ID and its complex path to implementation and innovational change. Identity. Inf. Soc. **3**(1), 27–41 (2010)
12. Vasconcelos, A., The Portuguese Interoperability Framework applied to the Portuguese Citizen Card Project. OECD Workshop on Digital Identity Management (IDM), May 9, 2007 (2007). http://www.oecd.org/dataoecd/36/9/38573902.pdf
13. Martens, T.: Electronic identity management in Estonia between market and state governance. Identity Inf. Soc. **3**(1), 213–233 (2010)
14. Tejchman, J., Kozicki, J.: Introduction: conceptual framework and research design for a comparative analysis of national eID Management Systems in selected European countries. Identity Inf. Soc. **3**, 1–2 (2010)
15. Nemzeti Adó- és Vámhatóság, Tájékoztató az adóügyek elektronikus úton történő intézéséhez. 32. számú információs füzet (2013). http://nav.gov.hu/nav/regiok/kiemeltadozok/aktualis/adougyek_32.html
16. Molnár, B., et al.: Identity-background checking: a solution, which Meets the requirements of privacy and personal data protection at identity management domain. SEFBIS Journal No.1, 22–32 (2006)
17. Shrivastava, S., Saquib, Z., P., G., Chomal, P.: Unique identity enabled service delivery through NSDG. In: Kő, A., Leitner, C., Leitold, H., Prosser, A. (eds.) EDEM 2012 and EGOVIS 2012. LNCS, vol. 7452, pp. 103–111. Springer, Heidelberg (2012)
18. Zwattendorfer, B., Zefferer, T., Tauber, A.: The prevalence of SAML within the european union. In: 8th International Conference on Web Information Systems and Technologies (WEBIST), pp. 571–576 (2012)