ИНФОРМАТИКА И КОМПЮТЪРНИ НАУКИ
INFORMATICS AND COMPUTER SCIENCES

TECHNOLOGICAL MODEL OF THE FIRST BULGARIAN NOTIFIED PRIVATE SCHEME FOR ELECTRONIC IDENTIFICATION THROUGH A MOBILE DEVICE

Konstantin Bezuhanov
University for Library Studies and Information Technologies

Abstract: *This paper presents a comprehensive examination of the first Bulgarian notified private scheme for electronic identification (eID) via mobile devices. It delves into the technological framework and operational mechanisms that align with the European Union's eIDAS regulation. The focus is on the innovative approach adopted by Bulgaria in establishing a private eID scheme, highlighting its compatibility with EU standards for cross-border electronic transactions. By analyzing the legal framework, technological infrastructure, and the notification process under eIDAS, this study showcases the scheme's significance in enhancing digital security and facilitating seamless digital services across the EU. The Evrotrust eID scheme, as a pioneering model, illustrates the practical application of advanced technologies in user registration and real-time electronic identification, ensuring high levels of security and user convenience. The findings contribute to understanding the dynamics of deploying private eID schemes within the EU's digital single market, emphasizing the role of national regulatory bodies and independent conformity assessment. This study underscores the potential of private eID schemes in driving digital transformation and fostering a secure digital environment.*
Keywords: *Electronic Identification, eIDAS Regulation, Mobile Devices, Digital Security, private scheme*

ELECTRONIC IDENTIFICATION AND NOTIFICATION OF EID MEANS

The identification of subjects is utmost important element for the functioning of society. It is necessary both for the provision of commercial services – banking, telecommunications, leasing, insurance, etc., and for the provision of administrative services by the state. It is also the basis for the functioning of the entire judicial system.

One of the key principles of the cornerstone regulatory act in the European Union and directly applicable to Bulgaria is Regulation (EU) No. 910/2014 of the European Parliament and of the Council of July 23, 2014 on electronic identification and trust services in electronic transactions on the Internal Market and on repealing Directive 1999/93/EC (eIDAS). This regulation establishes the principle of mutual recognition in Art. 7. This comes to say that if means for electronic identification are recognized as compatible with eIDAS standards in one EU Member State, they must be recognized as valid in all other Member States. eIDAS is interested in and regulates the use of electronic identification only for online access to public services. It does not regulate

electronic identification in the private sector. There, each private entity is free to choose any method it wishes for the electronic identification of its customers and counterparties. Also, eIDAS does not establish a single means of electronic identification of European citizens and organizations. Each Member State has the freedom to choose which technology and which model of electronic identification it will prefer (Sharif et al. 2022).

The process of officially "recognizing" a national scheme at EU level to be usable cross-border is called "notification". Each country decides for itself which schemes to notify. eIDAS allows the notification of public and private electronic identification schemes (eIDAS Regulation, Preamble (13). Bulgaria, as a member state of the EU, has allowed pluralism in the choice of national schemes for electronic identification.

Pursuant to Decision 634/27.08.2021 of the Council of Ministers of the Republic of Bulgaria, providers of qualified authentication services who have entered an electronic identification service in the National trust list of authentication services as services at the national level may request from the Minister of e-Government to be notified the electronic identification schemes built by them, if they meet the requirements of Art. 7–9 of eIDAS.

The supervisor of the private eID scheme providers is the Communications Regulation Commission. It oversees providers of electronic identification services, as a type of trust service, in accordance with eIDAS and the Electronic Document and Electronic Trust Services Act. The CRC grants or revokes qualified status to the trust service providers and to the trust services they provide, in accordance with Art. 20 and 21 eIDAS. CRC is also responsible for establishing, maintaining and publishing the National List of Trust Services, pursuant to Art. 22, paragraph 3 of eIDAS (eIDAS, Art. 32, para. 4).

The assessment of whether the electronic identification scheme and means of electronic identification meet the requirements of eIDAS and whether the scheme is suitable for notification is based on the verification and certification by an independent conformity assessment body. Regarding the notification obligation, the Minister of e-Government is subordinate and reports to the Council of Ministers.

The Minister of e-Government has published a special Methodology for the verification of electronic identification schemes. Based on this Methodology, any eID scheme provider willing to have its scheme notified as national, must submit an application which is assessed by an interagency committee.

Providers of private electronic identification schemes in Bulgaria must meet a number of technical and organizational requirements, as well as comply with certain procedures. The same are described in the internal rules of the electronic identification service providers.

Among the requirements that must be met, those for the security of the systems, for the protection of personal data (Dimitrov & Zahariev 2022, 239–256) and for risk management should be noted. Providers of private electronic identification schemes must also ensure that their systems are compatible with the technological requirements of public bodies that provide electronic services (Alonso et al. 2020, 770).

After successfully passing through the internal national evaluation procedure, the state, through the Minister of e-Government, notifies the European Commission according to the procedure provided for in eIDAS.

Currently, only one Bulgarian provider of an electronic identification scheme has successfully passed an inspection by the European Commission for compliance of the scheme with the requirements of eIDAS and has successfully completed the notification procedure – "Eurotrust Technologies" AD. It is listed in the EU Trust List of the Pre-notified and Notified National eID schemes (European Commission, n.d.).

MECHANISM OF OPERATION OF THE BULGARIAN NOTIFIED PRIVATE SCHEME FOR ELECTRONIC IDENTIFICATION EVROTRUST EID

The electronic identification scheme Evrotrust eID is a complex system for electronic identification of individuals and legal entities, which includes users, relying parties, infrastructure, hardware and software components, connectivity to registries and other components, providing secure electronic data verification in real time for the needs of providing electronic services. It is based on the requirements of eIDAS.

The scheme consists of two main processes:

- remote user registration;
- issuing a means of electronic identification in real time to a user (electronic identification service) and providing the means of electronic identification to a relying party.

Remote user registration

For the remote registration of a user, an identification method is used, which is certified by an accredited conformity assessment body for compliance with the requirements of Art. 24, para. 1, "d" of eIDAS, as a method giving a degree of assurance at to a physical presence. The method is nationally recognized by the national regulatory body at the place of establishment of "Eurotrust Technologies" AD – the CRC, and it was given a qualified status by the Decision of CRC with Ex. No. 12-01-1758 of 29.12.2020 (European Commission, n.d.).

In order to initiate the remote registration process, the user needs to install the Evrotrust application on their mobile phone as a stand-alone application or integrated via an SDK module into a mobile application of a relying party. For the purposes of registration, it is necessary for the person to capture a photo of his identity document with the camera of his mobile phone. The data obtained from the machine-readable area of the identity document and the image of the document are processed automatically, including being checked for security elements by specialized software. The scheme is developed using technology that automatically recognizes the data from the identity document and checks it against a trusted source (for example: population register, identity document register, etc.) through an encrypted real-time connection. When the person is a legal entity, the attributes of the legal entity and its status, together with the representative power, are verified by the relevant national register of legal entities (in Bulgaria – Commercial Register and the Register of Non-Profit Legal Entities maintained by the Registration Agency). When no direct connectivity is established and the ID document is digital and has an embedded RFID ICAO chip and the mobile device supports NFC technology, the data is extracted from the ID document by bringing it closer to the mobile device.

After the data is retrieved and verified, an electronic identification process begins to verify that the person providing the ID document is identical to the person identified by the validated ID document. The process is automated and includes automatic video identification, which prompts the person to video-capture their face with the front-facing camera of the mobile device, while performing an automated analysis of the facial image with the acquired and verified biometric data from the face photo from the ID document. The result is generated by high-tech software that performs biometric analysis of the shape and unique features of the face with a high degree of matching, and the process also includes a 3D verification of the presence of a live person in front of the camera through a specially integrated technology (Lee et al. 2008). This allows to avoid using someone else's photo, video or computer generated avatar of another person.

To establish the identity of a natural person who is a representative of a legal entity (managers, board members, procurators, etc.), when the representative power derives from law, an automated check is made against the relevant registers in the presence of such integration (for example:

Commercial register, Register of non-profit legal entities, etc.).

In case of unsuccessful automatic video identification (for example, due to possible changes to the face or the photo was not received from a reliable source), the process switches to video identification by an operator of "Eurotrust Technologies" JSC through an established video connection between the user's mobile device and the operator. The real-time video session operator visually identifies the person based on the copy of the ID document and the extracted photo, asking the person control questions to establish permanent knowledge of certain personal data, as well as prompting the person to turn the camera to capture the document for identity verification of security and other elements (Dimitrov, 2023).

Any identification, whether automated or done by an operator, is subject to an immediate follow-up second check by a supervisor.

After successful identification of the person, a profile is created and he can be issued a means of electronic identification and provided with qualified trust services (Evrotrust, 2023).

Electronic identification service

The electronic identification service is a complex service for attesting the electronic identity of a user registered under item 1, which is provided in real time. It consists of the following steps:

Request for identification

The user accesses a system of a trusted party (e.g. a public service) for which there is a need for electronic identification. After submitting an identifier (e.g. national identity number, registered mobile number or registered e-mail), the system of the relying party submits a request for user identification to the backend system of "Eurotrust Technologies" JSC. The request states the amount of personal data required from the user for identification purposes for the specific public service. The request is automated, in machine-readable form, and can be submitted via an API for automated connectivity or through a purpose-built portal from which a relying party representative can initiate the request via a web interface. A national uniform identification code is also provided for the identification of a legal entity.

User verification and authentication

The request for electronic identification is received by "Eurotrust Technologies" JSC, and after verifying the fact that there is a registered user with a corresponding ID of the person, an immediate ("instant") message is sent in the mobile application. The user opens the request and is informed that identification is requested, while is also advised on who has requested the identification, as well as the purposes of the identification (which service it is meant for), including the volume of personal data that is required for the identification. If identification of a legal entity is requested, information on the required data of the legal entity is also provided. If the user agrees to enable the electronic identification service, he confirms the identification by authenticating with knowledge (PIN code) or biometrics (face, thumbprint, etc.) (Zahariev, 2018) accessible through the smart device.

Issuing a means of electronic identification

Upon informed confirmation of the desire for identification and activation of the electronic identification service, a means of electronic identification is issued subject to compliance with the following rules:

A. In the presence of established connectivity with primary registers (national registers for identity documents, population databases, commercial registers, etc.) a check is carried out for the actuality and validity of the data at the time of identification;

B. Based on the validated data, an electronic document is generated for the user – a statement for the provision of personal data. This document is in both human-readable (PDF) and machine-readable (XML) format, in which the user makes a statement that this is their personal data required by the relying party and that it is up-to-date. For legal entities, a second document is generated in the same formats, in which a statement is made about the data of the legal entity and the relationship between the individual and the legal entity.

C. A key pair is generated at the request of the user remotely in a hardware cryptographic module (HSM), for an advanced or for a qualified electronic signature;

D. An attribute qualified or advanced certificate is issued for the public key, which contains those personal data that are required under the Implementing Regulation (EU) 2015/1501. Thus, it is possible to verify the identity between data declared and authenticated in the attributive certificate and confidence in the authenticity of the declared data. Upon identification of a legal entity, a statement is generated in which data about it is entered, and an attributive qualified or advanced certificate is issued;

E. The private key of the key pair is used to remotely sign the privacy statement in the relevant standard in the hardware cryptographic module, with the attributive certificate accompanying the signed document. For the legal entity, the document containing the data on the legal entity is also signed remotely. "Eurotrust Technologies" JSC is certified by an independent conformity assessment body under eIDAS for the service of remote signing with an advanced or qualified electronic signature, according to the requirements of the European standards;

F. A qualified electronic time stamp will be then issued for the statement of disclosure of personal data so signed, which shall also be attached to the statement. Such is generated and attached to the statement of provision of data for the legal entity;

G. The electronic identification means is generated consisting of the personal data disclosure statement in PDF/XML format, signed with an advanced or qualified electronic signature, accompanied by an attributive qualified or advanced certificate and a qualified electronic time stamp. It this sent to the relying party through an automated interface (API) or through a portal operated by a representative of the relying party. For the legal entity, the means of electronic identification for the legal entity is also added in a package (Dimitrov, 2023).

The mechanism of action of the electronic identification scheme is depicted in the following diagram:

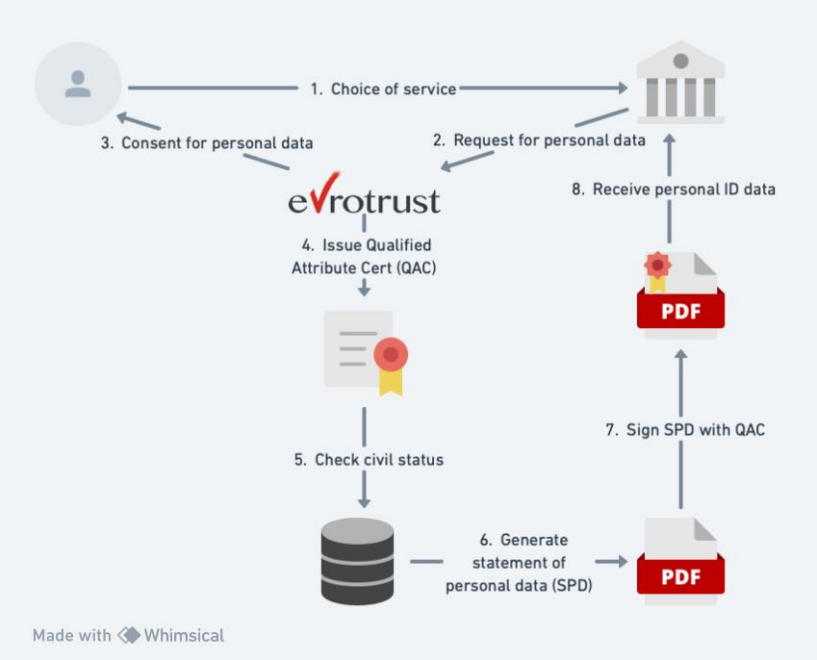

Fig. 1. Mechanism of the private notified electronic identification scheme Evrotrust eID

EVROTRUST EID ASSURANCE LEVELS

The electronic identification scheme of "Eurotrust Technologies" AD is built on a dynamic model for authentication of data that can be provided depending on the volume requested by the relying party.

The minimum set of data to be attested for a natural person are: surname (or names), first name (or names), date of birth, national unique identifier, if any, in accordance with the technical specifications for cross-border identification purposes, which will remain unchanged for as long as possible (for example, for Bulgarian citizens and foreigners residing in Bulgaria, the EGN, respectively LNC). The specified minimum data set is always verified with a significant or high level of confidence. Additional specific data that may be submitted are, for example: first name (or names) and surname (or names) at birth, place of birth, permanent address, gender, current address, as well as any other data that may be supplemented indefinitely and dynamically and be authenticated to the relying party (e.g. data related to owned identity document, professional identity, health status, medical status, educational status, geolocation, etc.).

For a legal entity, the minimum set of data to be authenticated is a name and a unique national identifier (in Bulgaria – EIC/BULSTAT). If necessary and upon request, additional and specific data can be certified, such as: VAT registration number, tax number, identification code according to Art. 3, par. 1 of Directive 2009/101/EC of the European Parliament and of the Council, the identification code of the legal entity (UEI) referred to in Commission Implementing Regulation (EU) No. 1247/2012; economic operator identification number (EORI number) specified in Commission Implementing Regulation (EU) No. 1352/2013; excise number provided for in Article 2, paragraph 12 of Council Regulation No. 389/2012, registered office, address of management, as well as any other data such as subject of activity, capital, representation, entry number in primary register, date of entry, management, method of representation, status (active, in liquidation, in bankruptcy), etc. (Dimitrov, 2023).

The additional specific data for both individuals and legal entities can be of different levels of assurance - high, substantial and low, depending on whether they have been checked by Eurotrust Technologies JSC against an authoritative source, they have been checked to a limited extent or are self-declared. The degree of security of any data can be entered into the means of electronic identification.

REFERENCES

Alonso, Á., A. **Gordillo,** A. **Pozo,** S. **López-Pernas,** L. **Marco** & E. **Barra** (2020). Enhancing University Services by Extending the eIDAS European Specification with Academic Attributes. *Sustainability*, [online] 12(3), 770. Available from: https://doi.org/10.3390/su12030770.

Dimitrov, G. (2023). *Legal Regime of Digital Transformation. Electronic Identification. Electronic Documents. Electronic Trust Services.* Sofia: Law and Internet Foundation.

Dimitrov, G., M. **Zahariev** (2022). Cyber Law in Bulgaria, Kluwer Law International BV, The Netherlands.

European Commission (n.d.). Overview of pre-notified and notified eID schemes under eIDAS. [online] Available from:https://ec.europa.eu/digital-building-blocks/sites/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS.

European Union (2014). Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (eIDAS Regulation). *Official Journal of the European Union*, L257/73. [viewed on 05 February 2024]. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014R0910 [Accessed: date].

Electronic Document and Electronic Trust Services Act (EDETSA) Article 32, paragraph 4.

Government of Bulgaria (2021). Методика за извършване на проверка на схеми за електронна идентификация. [viewed on 03 February 2023]. Available from: https://e-gov.bg/wps/wcm/connect/e-gov.bg-18083/f9cc3d89-984b-4861-98e3-f2a62cec7644/Методика+проверка_частни+схеми+е-идентификация_+08+11+2021.pdf?MOD=AJPERES&CONVERT_TO=url&CACHEID=ROOTWORKSPACE.Z18_PPGAHG800HDT40Q9L5OQ9M3000-f9cc3d89-984b-4861-98e3-f2a62cec7644-nSQr4wA.

Lee, H., S.-H. **Lee,** T. **Kim** & H. **Bahn,** (2008). Secure User Identification for Consumer Electronics Devices.

Sharif, A., M. **Ranzi,** R. **Carbone,** G. **Sciarretta,** F. A. **Marino** & S. **Ranise,** (2022). The eIDAS Regulation: A Survey of Technological Trends for European Electronic Identity Schemes. *Applied Sciences*, [online] 12(24), 12679.

Overview of Pre-Notified and Notified EID Schemes Under EIDAS. [viewed on 07 February 2024]. Available from: https://ec.europa.eu/digital-building blocks/sites/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS.

The Registration Process Video (n.d.). [viewed on 25 September 2023]. Available from: https://youtu.be/DZAIyxuQu88?si=uajbkv69lVJbuuKu.

Zahariev, M. (2018). Automated Profiling and the Personal Data Protection, Analysis of GDPR, Sofia: Za bukvite – O pismeneh.

ТЕХНОЛОГИЧЕН МОДЕЛ НА ПЪРВАТА БЪЛГАРСКА ЧАСТНА СХЕМА ЗА ЕЛЕКТРОННА ИДЕНТИФИКАЦИЯ ЧРЕЗ МОБИЛНО УСТРОЙСТВО

Резюме: *Настоящата статия представя цялостно изследване на първата частна схема, нотифицирана за електронна идентификация (EID) чрез мобилни устройства. Статията задълбочава в технологичната рамка и оперативните механизми, които се привеждат в съответствие с регулацията на EIDAS на Европейския съюз. Фокусът е върху иновативния подход, възприет от България при създаването на частна схема на EID, като подчертава съвместимостта му със стандартите на ЕС за трансгранични електронни транзакции. Анализирайки правната рамка, технологичната инфраструктура и процеса на уведомяване по EIDAS, това проучване показва значението на схемата за повишаване на цифровата сигурност и улесняване на безпроблемните цифрови услуги в ЕС. Схемата на Evrotrust EID, като новаторски модел, илюстрира практическото приложение на модерни технологии в регистрацията на потребителите и електронната идентификация в реално време, като*

гарантира високи нива на сигурност и удобство на потребителя. Констатациите допринасят за разбирането на динамиката на разгръщането на частни схеми на EID в рамките на дигиталния пазар на ЕС, подчертавайки ролята на националните регулаторни органи и независимата оценка на съответствието. Това проучване подчертава потенциала на частните схеми на EID при стимулиране на цифровата трансформация и насърчаване на сигурна цифрова среда.

Ключови думи: *електронна идентификация, Регламент EIDAS, мобилни устройства, цифрова сигурност, частна схема*

Konstantin Bezuhanov, PhD candidate
University of Library Studies and Information Technologies
E-mail: kbezuhanov@gmail.com