# ЕДИНАЯ ИДЕНТИФИКАЦИЯ ФИЗИЧЕСКИХ ЛИЦ

*Шуманский Д.И.*

*Научно-производственное республиканское унитарное предприятие «Научно-исследовательский институт технической защиты информации»*
*г. Минск, Республика Беларусь*

*Пулко Т.А. – канд. техн. наук, доцент*

Система единой идентификации (СЕИ) разрабатывается с целью формирования единых подходов к обеспечению идентификации гражданина с использованием информационно-коммуникационных технологий и обеспечения юридически значимого электронного взаимодействия между гражданами и государством (за счет реализации возможности совершения юридически значимых действий посредством ЭЦП) и предназначена для предоставления информационным системам различных государственных органов и иных организаций Республики Беларусь сервиса идентификации/аутентификации. Сервисом может воспользоваться любая зарегистрированная в СЕИ информационная система. СЕИ должна предоставлять информационным системам (ИС) различных государственных органов и иных организаций Республики Беларусь сервисы аутентификации, реализованные на основе спецификации OIDC с использованием криптографических алгоритмов, определенных в государственных стандартах Республики Беларусь.

Аутентификацию может пройти любой пользователь, являющийся владельцем криптографического токена, в том числе содержащегося на идентификационной карте (КТА), или средством криптографической защиты информации, которое реализует функцию выработки ЭЦП (средство ЭЦП).

В ходе аутентификации пользователь должен выбрать средство для аутентификации, а также в качестве кого он хочет пройти процедуру аутентификации: физического лица, представителя физического лица или представителя юридического лица.

Для обеспечения аутентификации секреты аутентификации пользователя хранятся в его КТА или средстве ЭЦП. Должна обеспечиваться конфиденциальность и целостность идентификационных и других данных пользователя, передаваемых в ходе аутентификации.

СЕИ обеспечивает информационное взаимодействие ИС с информационными системами, являющимися источниками данных сервера ресурсов, посредством Общегосударственной автоматизированной информационной системы (ОАИС).

СЕИ обеспечивает централизацию процесса идентификации и аутентификации пользователей с использованием КТА или средства ЭЦП. СЕИ ведет аудит событий, связанных с выпуском, регистрацией, использованием, перевыпуском, выводом из эксплуатации билетов аутентификации (БА) и билетов доступа (БД).

СЕИ обеспечивает получение информационного запроса от ИС на получение ресурсов пользователя, определение по адресному справочнику адреса нахождения соответствующего ресурса и направление запроса через ОАИС, после получения информации из информационной системы посредством ОАИС, предоставление информации запрашивающей ИС.

СЕИ строится с использованием протокола, описанного в спецификации OpenID Connect. Для обеспечения безопасности передаваемых персональных данных и секретов аутентификации применяются криптографические алгоритмы, обеспечивающие генерацию псевдослучайной числовой последовательности, предварительное шифрование, выработку и проверку электронной ЭЦП стандартизованные в Республике Беларусь. Для выполнения протокола аутентификации и обеспечения взаимодействия с КТА и средством ЭЦП разрабатывается клиентская программа.

**Список использованных источников:**

1. ТР 2013/027/BY «Информационные технологии. Средства защиты информации. Информационная безопасность»
2. СТБ 34.101.21-2009 «Информационные технологии. Интерфейс обмена информацией с аппаратно-программным носителем криптографической информации (токеном)»
3. СТБ 34.101.23-2012 «Информационные технологии и безопасность. Синтаксис криптографических сообщений»
4. СТБ 34.101.31-2011 «Информационные технологии. Защита информации. Криптографические алгоритмы шифрования и контроля целостности»
5. СТБ 34.101.45-2013 «Информационные технологии и безопасность. Алгоритмы электронной цифровой подписи и транспорта ключа на основе эллиптических кривых»
6. СТБ 34.101.47-2017 «Информационные технологии и безопасность. Криптографические алгоритмы генерации псевдослучайных чисел»
9. СТБ 34.101.79-2019 «Информационные технологии и безопасность. Криптографические токены»
10. РБ.ЮСКИ.19003-01 91 01 «Профиль КТА»
11. Бердникова Ю.Н. «Белорусская интегрированная сервисно-расчетная система, как элемент электронной трансформации государственных административных процессов и услуг»
12. RFC 2616 Hypertext Transfer Protocol – HTTP/1.1
13. Спецификация OpenID Connect Core 1.0
14. RFC 2616 Hypertext Transfer Protocol -- HTTP/1.1
15. RFC 6749 The OAuth 2.0 Authorization Framework
16. RFC 6750 The OAuth 2.0 Authorization Framework: Bearer Token Usage
17. RFC 7636 Proof Key or Code Exchange by OAuth Public Clients