МРНТИ 50.41.23
https://doi.org/10.56132/2791-3368-2026-1-65-83-94

Ж.С. Есенгалиева[1], О.А. Усатова[2], С. Жумаханов[2]
[1]L.N. Gumilyov Eurasian National University, Астана, Казахстан,
[2]Institute of Information and Computational Technologies CS MSHE RK, Алматы, Казахстан
E-mail: olgaussatova@gmail.com

РАЗРАБОТКА ИНТЕГРАЦИОННОГО ПРОГРАММНОГО МОДУЛЯ ДЛЯ ОРГАНИЗАЦИИ ЗАЩИЩЁННОГО ОБМЕНА ДАННЫМИ МЕЖДУ ИНФОРМАЦИОННЫМИ СИСТЕМАМИ

Аннотация. В статье рассмотрена платформа Смарт Бридж (Smart Bridge), которая предназначена для интеграции конфиденциальной информации между программными продуктами государственных структур и бизнеса, обеспечивая безопасный и стандартизированный обмен данными. В целях интеграции данных между интеллектуальной антикоррупционной системой защиты информации и валидации учебных достижений, а также официальных документов студентов, курсантов и выпускников вузов, военных учебных заведений Республики Казахстан и ведомственными информационными системами разработана архитектура взаимодействия с шиной электронного правительства. Предлагаемый программный модуль предназначен для получения сведений о физических лицах из государственной базы данных физических лиц (ГБД ФЛ) через шлюз электронного правительства. Взаимодействие осуществляется в формате SOAP-сообщений с использованием электронной цифровой подписи для обеспечения подлинности и целостности данных.

Таким образом, предложен сервис, вызываемый в процессе регистрации на портале студента, курсанта или выпускника с применением электронной цифровой подписи, реализованный с помощью платформы Smart Bridge.

Ключевые слова: электронная цифровая подпись, электронное правительство, SOAP-сообщение, Smart Bridge, XML-запрос.

Введение.

С развитием интернет-технологий, совершенствуются электронные механизмы, такие как электронное правительство, электронная коммерция, электронные фондовые рынки, образовательные порталы и т.д., где все необходимые данные транспортируются по сетевым технологиям. При этом важную роль для обеспечения целостности, подлинности и неопровержимости передаваемой электронной информации играют электронные цифровые подписи.

Электронная цифровая подпись (ЭЦП) представляет собой данные, которые криптографически зашифрованы и способны авторизировать, идентифицировать физическое либо юридическое лицо, при этом полностью эквивалентно ручной подписи в электронных документах, на сайтах образовательных, государственных, ведомственных, медицинских, банковских и других услуг. Данный электронный механизм способствует безопасности от несанкционированного доступа.

В рамках разработки интеллектуальной антикоррупционной системы защиты информации, валидации результатов учебных достижений, официальных документов студентов, курсантов и выпускников высших учебных заведений, высших военно-учебных заведений Республики Казахстан для обеспечения информационной безопасности использование электронной цифровой подписи играет немаловажную роль.

Рассмотрим актуальность исследования на опыте предшественников в области использования электронных цифровых подписей. Нами проведен обзор 1388 статей из различных научных баз данных по ключевому слову «электронная цифровая подпись». Критерии сортировки: отобраны именно статьи за период 2020-2026гг., язык написания английский. Далее, отбор был осуществлен по абстрактам и наиболее релевантные, цитируемые, на наш взгляд, работы представлены ниже.

В исследовании [1] описан алгоритм для подписания электронных цифровых подписей на документах с целью проверки подлинности личности на основе пиксельных данных. Предложенный авторами метод нацелен на минимизацию обработки данных при извлечении небольшой части пиксельных данных, при этом используются уравнения из китайской теоремы об остатках, для дальнейшей оптимизации времени обработки.

В статье [2] рассматривается значение цифровой подписи в электронной коммерции. Интернет и электронная коммерция открывают множество новых возможностей для потребителя, рассматривается безопасность (или предполагаемое отсутствие безопасности) обмена личными и финансовыми данными.

В работе [3] отраслевой сферы обмена использованы архивные данные за определенный период, с целью легитимации цифровых подписей в электронных транзакциях посредством законодательства.

Авторы в своих трудах [4] отмечают, то в процессе работы с компьютерами обеспечение законности, отслеживаемости, защиты от подделки и уникальности документов является важной частью развития компьютерных технологий. Для обеспечения безопасности в процессе аутентификации электронных контрактов в данном исследовании был проведен детальный анализ и разработана технология электронной подписи. В этом исследовании объединены технологии PKI и USB-ключей. Усовершенствованная технология электронной подписи в данном исследовании повышает безопасность подписания электронных контрактов на рабочем месте.

Существующие схемы цифровой подписи, основанные на теоретико-числовом предположении, уязвимы для квантовых атак из-за развития квантовых компьютеров. Авторы подробно описывают [5] необходимость в схеме цифровой подписи, устойчивой к квантовым компьютерам, то есть в постквантовой цифровой подписи. Многомерная криптография с открытым ключом является одним из наиболее перспективных кандидатов в постквантовую криптографию, поскольку конструкции на ее основе являются вычислительно быстрыми и требуют лишь умеренных вычислительных ресурсов.

В статье [6] рассматривается развитие «умных городов» посредством электронного правительства. При этом существующие системы электронного правительства сталкиваются с такими проблемами, как избыточность данных и нарушения конфиденциальности в процессе аутентификации. Для решения этих проблем в данном исследовании предлагается инновационная схема аутентификации, основанная на электронных идентификационных картах (eID) и смарт-контрактах на основе блокчейна. Пользователи генерируют цифровые подписи с помощью eID-карт, а смарт-контракт автоматически проверяет действительность подписи и статус сертификата. Анализ производительности и безопасности показывает, что данная моель эффективно противостоит распространенным атакам и минимизирует риски утечки конфиденциальной информации, значительно повышая практическую безопасность систем электронного правительства.

В трудах [6] представлена FIBS: быстрая цифровая подпись на основе изогений, использующая хеш-функцию на основе изогений. Авторы объединяют хеш-функцию CGL и SPHINCS+ – алгоритм цифровой подписи на основе хеширования. Результаты показывают, что FIBS обеспечивает «умеренно быструю и эффективную» производительность среди цифровых подписей на основе изогений, сохраняя при этом простоту и легкость реализации.

Таким образом, в научной литературе широко освещается тема защиты данных посредством электронных цифровых подписей. Технологии совершенствуются, очень много работ по постквантовым электронным цифровым подписям, представлены различные методы защиты конфиденциальных данных субъектов электронной деятельности.

Материалы и методы.

В качестве материалов в данном исследовании использована платформа Смарт Бридж (Smart Bridge). Данная платформа предназначена для интеграции между информационными системами государственных структур и бизнеса, позволяет подключиться к необходимым сервисам, предоставляет статистику запросов, завершенных интеграций за определенный период, предоставляет инструкции, а также позволяет проверить валидацию схем XSD и запросов/ответов, демонстрирует этапы процессов интеграции. Платформа служит в качестве умного моста между государственной базой

данных физических лиц и базой данных контроля доступа к персональным данным, когда пользователь вводит только персональный идентификационный номер, затем остальные данные подгружаются с государственных информационных систем.

Smart Bridge – это информационно-коммуникационная услуга в виде платформы «Витрина сервисов», направленная на упрощение процессов интеграции информационных систем между государственными структурами и частным бизнесом, способствуя более эффективному обмену информацией и улучшению общей прозрачности и координации.

В работе рассматривается модуль контроля доступа к персональным данным (КДП).

Модуль КДП предназначен для интеграции корпоративных и государственных информационных систем с сервисом контроля доступа к персональным данным, функционирующим на платформе SmartBridge. Основная цель модуля — обеспечить безопасный, юридически значимый и автоматизированный обмен данными, связанными с запросами на получение персональных сведений граждан по их ИИН (индивидуальному идентификационному номеру).

Модуль реализует следующий алгоритм взаимодействия:

– формирование запроса в формате XML в соответствии с утверждённым шаблоном SmartBridge;

– подписание запроса ЭЦП организации (ЭЦП юридического лица или сотрудника);

– отправку запроса в веб-сервис КДП;

– получение и разбор SOAP-ответа, включая извлечение кода верификации и публичного ключа;

– обработку статусов доступа, ошибок и уведомлений.

Платформа Smart Bridge предназначена для получения сведений о физических лицах из государственной базы данных физических лиц (ГБД ФЛ) через шлюз электронного правительства (ШЭП). Взаимодействие осуществляется в формате SOAP-сообщений с использованием электронной цифровой подписи для обеспечения подлинности и целостности данных.

Результаты и обсуждение.

В ходе исследования разработана архитектура подключения персональных данных через платформу SmartBridge, представленная на рисунке 1. Архитектура модуля КДП состоит из нескольких логических компонентов:

1) KDPRequest - Формирование XML-запросов на получение персональных данных и на проверку статуса.

2) KDPResponce - Парсинг SOAP-ответа, обработка результата, определение статуса и извлечение полезных данных.

3) SignHelper - Подписание XML-документов ЭЦП, обеспечение криптографической подлинности.

4) DATASTATUS - Перечисление возможных статусов обработки запроса.

5) KDPSettings, CompanySettings, SenderInfoSettings, ECPSettings - Классы конфигураций, содержащие параметры интеграции, ЭЦП и идентификаторы организации.

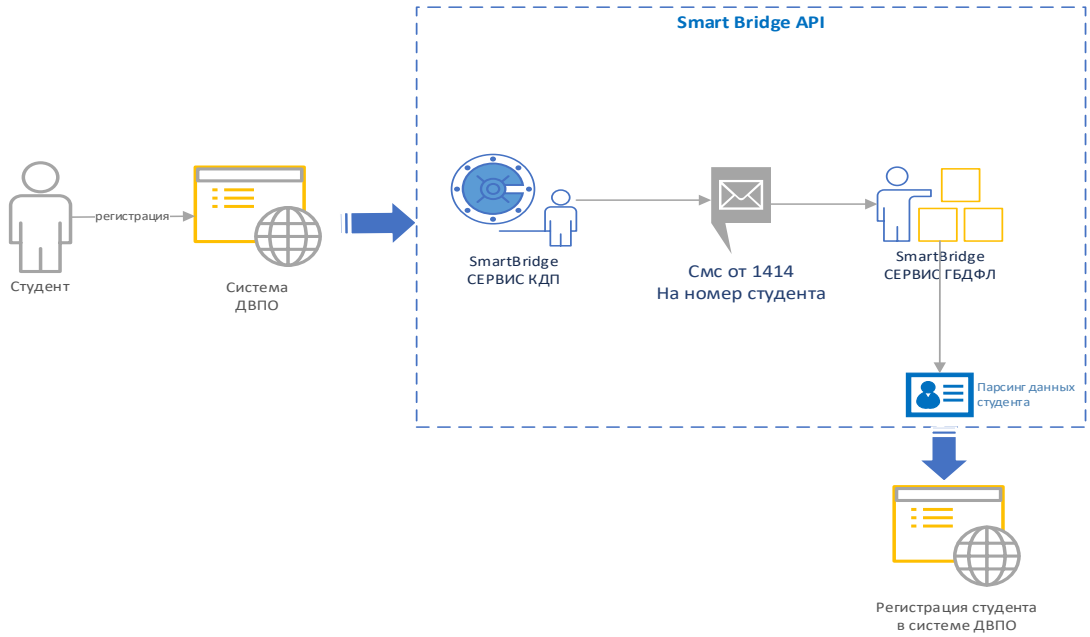

Рисунок 1 – Архитектура подключения к платформе SmartBridge

Как отмечено выше, взаимодействие осуществляется в формате SOAP-сообщений с использованием электронной цифровой подписи для обеспечения подлинности и целостности данных. Формирование XML-запроса представлено на рисунке 2, где используется XML-шаблон, в который динамически подставляются значения параметров запроса.

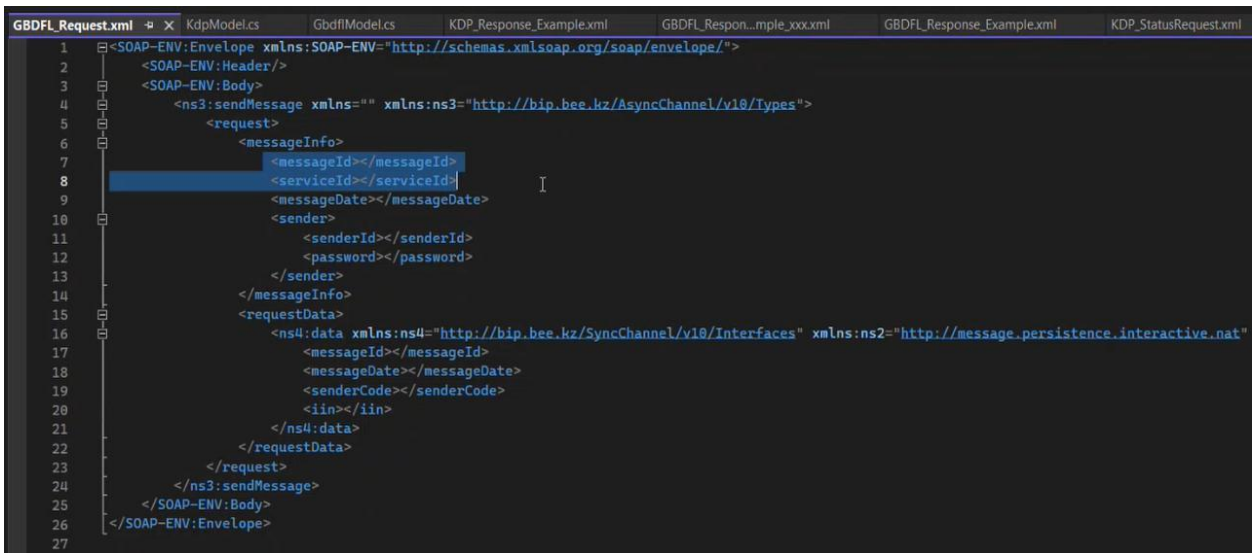

Рисунок 2 – Формирование XML-запроса

Платформа Swagger, в данном случае позволяет произвести связь между различными программными приложениями и автоматически осуществлять генерацию документации. Назначение сервисов Swagger описаны ниже и представлены на рисунке 3.

Представленные сервисы (KDP, GBDFL) способствуют проверке подлинности запрашиваемых данных. Первый запрос KDP предоставляет доступ, в результате которого получаем токен, и далее в сервисе GBDFL вставляется полученный ранее токен, в итоге генерации документации, соответствующие данные по физическому лицу, будут предоставлены.

В модуле контроля доступа к персональным данным поддерживаются следующие параметры:

1) MessageId - Уникальный идентификатор запроса (GUID).
2) SessionId - Идентификатор текущей сессии.
3) MessageDate - Дата и время отправки запроса в формате ISO 8601.
4) Uin - ИИН субъекта персональных данных.

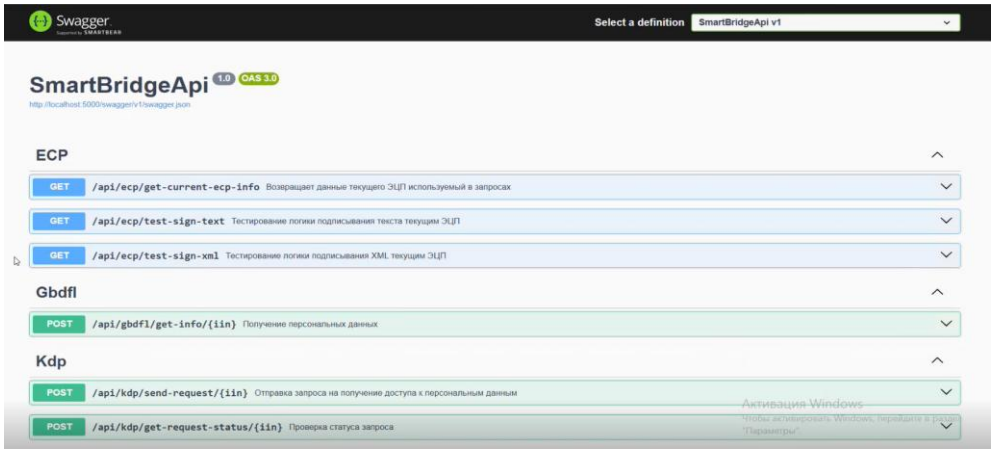

Рисунок 3 – Сервисы Swagger

Метод GetStatusXml() формирует аналогичный XML для проверки статуса ранее отправленного запроса.

Непосредственное подписание запросов ЭЦП перед отправкой XML-документа проходит обязательное криптографическое подписание с помощью модуля SignHelper, что в свою очередь обеспечивает юридическую подлинность, защиту данных. В процессе подписания производится загрузка ключей из контейнера ЭЦП, создаётся XML-подпись в соответствии с форматом XMLDSig, результат возвращается в виде подписанного XML-документа, готового к отправке.

Обработка ответа от КДП. Ответ от сервиса КДП поступает в виде SOAP-сообщения. Класс KDPResponce, представленный на рисунке 4 выполняет: разбор XML-документа; извлечение элементов данных (status, code, public-key); сопоставление статуса с перечислением DATASTATUS; формирование модели результата. Модуль КДП соответствует требованиям SOAP 1.1 / WS-Security и стандартам интеграции SmartBridge, EGOV.

```
{
    KDPResponce res = null;
    try
    {
        XDocument xml = null;

        xml = XDocument.Parse(response_data);

        XNamespace soap = "http://schemas.xmlsoap.org/soap/envelope/";
        XNamespace kdp = "http://service.2fa-chain.kz/ns/kdp";

        var body = xml.Descendants(soap + "Body").FirstOrDefault();
        if (body == null)
            throw new Exception("Ошибка парсинга ответа: SOAP Body не найден");

        var response = body.Element(kdp + "sendMessageResponse");
        if (response == null)
            throw new Exception("Ошибка парсинга ответа: sendMessageResponse не найден");

        var data = response.Descendants(kdp + "data").FirstOrDefault();
        if(data == null)
            throw new Exception("Ошибка парсинга ответа: data не найден");

        res = new KDPResponce();
        res.Status = Enum.Parse<DATASTATUS>(data.Element(kdp + "status")?.Value);
        res.Code = data.Element(kdp + "code")?.Value;
        res.PublicKey = data.Element(kdp + "public-key")?.Value;
    }
    catch (Exception ex)
    {
        throw ex;
    }
    return res;
}
```

Рисунок 4 – Фрагмент сервиса контроля доступа к персональным данным

Также нами предоставлен перечень статусов, описанный открытым пользовательским перечислимым типом public enum DATASTATUS, представленный в таблице 1.

Таблица 1 – Перечень статусов

Статус	Описание	Действие
VALID	Пользователь дал согласие, доступ разрешён.	Разрешить получение данных, сохранить код.
INVALID	Пользователь отказал в доступе.	Прекратить обработку.
PENDING	Ожидается подтверждение от субъекта (SMS или портал).	Поставить в очередь ожидания.
TIMEOUT	Время ожидания ответа истекло.	Повторить запрос.
NOT_FOUND	ИИН не найден в базе.	Сообщить об ошибке идентификации.
ERROR	Ошибка на стороне КДП.	Логировать и уведомить оператора.

При реализации предусмотрены логирование и обработка ошибок таких этапов как сохранение исходных XML-запросов и ответов, запись статусов запросов, протоколирование ошибок (например, при отсутствии шаблона, ошибке подписи, сетевых сбоях или некорректных ответах SOAP).

Модуль ГБДФЛ (Государственная база данных физических лиц) предназначен для интеграции с государственным сервисом, предоставляющим сведения об обучающихся, курсантах Республики Казахстан по их ИИН (индивидуальному идентификационному номеру).

Данный модуль представляет собой SOAP-сервис для получения официальных данных о физическом лице, включая:

– ФИО, дату рождения, пол;

– гражданство и национальность;

– место рождения;

– адрес регистрации и фактического проживания;

– документы (удостоверение личности, паспорт, свидетельство о рождении и др.).

Модуль GBDFL построен по принципу разделения ответственности и включает несколько ключевых компонентов, описанных в таблице 2.

В данном модуле формируется XML-запрос в основном классе для генерации запросов — GBDFLRequest. Он подставляет необходимые значения в XML-шаблон GBDFL_Request.xml, включая: идентификаторы запроса, дату и время отправки, реквизиты отправителя и организации, ИИН запрашиваемого физического лица.

Таблица 2 – Компоненты модуля GBDFL

Компонент	**Назначение**
GBDFLRequest	Формирует XML-запрос на получение данных о физическом лице по ИИН.
GBDFLResponce	Обрабатывает и парсит SOAP-ответ от сервиса.
Person	Модель, описывающая структуру данных о физическом лице.
SignHelper	Модуль, обеспечивающий подписание XML-документа ЭЦП.
CodeNameChange, Address, Document и др.	Дополнительные модели, описывающие атрибуты и составные элементы сведений о человеке.

Перед отправкой в SmartBridge XML-документ подписывается ЭЦП юридического лица или сотрудника организации, чтобы обеспечить его аутентичность и соответствие требованиям законодательства. Код представлен ниже (рисунок 5):

```
public string GetRequest(string iin, SenderInfoSettings senderInfoSettings, CompanySettings companySettings,
    GBDFLSettings gBDFLSettings, ECPSettings ecp)
{
    string signResult = string.Empty;
    try
    {
        this.MessageId = Guid.NewGuid().ToString();
        this.MessageDate = DateTime.Now;
        this.Iin = iin;
        string xml = this.GetXml(senderInfoSettings, companySettings, gBDFLSettings);

        SignHelper signHelper = new SignHelper(ecp);
        signResult = signHelper.SignXML(xml);
    }
    catch (Exception ex)
    {
        throw ex;
    }
    return signResult;
}
public string SignXML(string xml)
{
    string signedXml = null;
    try
    {
        kalkan.SignXML("", 0x00000004 | (int)KALKANCRYPTCOM_FLAGS.KC_WITH_CERT, "reqDataId", "requestData",
            "http://schemas.xmlsoap.org/soap/envelope/", xml, out signedXml);

        CheckLastError(kalkan, "SignXML");

        if (string.IsNullOrEmpty(signedXml))
            throw new Exception("Результат подписи пустой");
    }
    catch (Exception ex)
    {
        throw ex;
    }
    return signedXml;
}
```

Рисунок 5 – Код подписания ЭЦП

После подписания результат можно безопасно передавать по SOAP-протоколу через SmartBridge API.

Заключение.

Предложенный сервис используется для получения официальных данных о физических лицах в целях межведомственного электронного взаимодействия и может быть интегрирован в информационные системы государственных органов и организаций. Разработанный модуль вызывается в процессе регистрации на портале студента, курсанта или выпускника с применением ЭЦП. Для граждан РК процесс регистрации упрощен по причине наличия государственной базы данных физических лиц, откуда можно с помощью ИИН получить представленные в таблице сведения. Эти данные после первичного обращения в ГБДФЛ дублируются и в дальнейшем они применяются для заполнения блока персональных сведений в печатных формах документов об образовании.

Сегодня в Smart Bridge представлены сервисы Единой платформы высшего образования (ЕПВО), предоставляющие образовательные сведения, необходимые для цифрового реестра документов об образовании: данные

дипломов выпускников, академическая успеваемость студентов, курсантов, магистрантов, докторантов.

Финансирование. Данное исследование финансировалось Комитетом науки МНВО РК (программно-целевое финансирование на 2024-2026 годы ИРН BR24993014 «Разработка интеллектуальной антикоррупционной системы защиты информации и валидации результатов учебных достижений и официальных документов студентов и выпускников вузов РК».

ЛИТЕРАТУРА

1. Somsuk, K. (2024). The development of signing and verification methods for high-speed digital signatures on electronic official documents by using RSA cryptography. Cogent Engineering, 11(1). https://doi.org/10.1080/23311916.2024.2432513
2. Voiculescu Madalina Irena & Gramada Dragu Argentina. (2009). THE ELECTRONIC SIGNATURE. Analele Universităţii din Oradea. Ştiinţe economice, 4(1), 940–942.
3. Dahabiyeh, L., & Constantinides, P. (2022). Legitimating digital technologies in industry exchange fields: The case of digital signatures. Information and Organization, 32(1), Article 100392. https://doi.org/10.1016/j.infoandorg.2022.100392
4. Jia, Y., & Li, Z. (2022). Auxiliary System for Contract Signing Based on Electronic Signature Technology. Wireless Communications and Mobile Computing, 2022(1). https://doi.org/10.1155/2022/1221162
5. Kundu, N., Debnath, S. K., Mishra, D., & Choudhury, T. (2020). Post-quantum digital signature scheme based on multivariate cubic problem. Journal of Information Security and Applications, 53, Article 102512. https://doi.org/10.1016/j.jisa.2020.102512
6. Liu, L., & Omote, K. (2025). Efficient authentication system based on blockchain for E-government. PloS One, 20(12), e0336997. https://doi.org/10.1371/journal.pone.0336997
7. Kim, S., Lee, Y., & Yoon, K. (2025). Performance evaluation of isogeny-based digital signature algorithms: introducing FIBS—fast isogeny-based digital signature. The Journal of Supercomputing, 81(3), Article 468. https://doi.org/10.1007/s11227-025-06970-z

Жанна Есенгалиева, PhD, доцент, L.N. Gumilyov Eurasian National University, Астана, Қазақстан

Ольга Усатова, PhD, қауымдастырылған профессор, Institute of Information and Computational Technologies CS MSHE RK, Алматы, Қазақстан

Саят Жумаханов, магистр, Institute of Information and Computational Technologies CS MSHE RK, Алматы, Қазақстан

АҚПАРАТТЫҚ ЖҮЙЕЛЕР АРАСЫНДА ҚАУІПСІЗ ДЕРЕКТЕР АЛМАСУДЫ ҰЙЫМДАСТЫРУ ҮШІН ИНТЕГРАЦИЯЛЫҚ БАҒДАРЛАМАЛЫҚ ҚҰРАЛ МОДУЛІН ӘЗІРЛЕУ

Аңдатпа. Бұл мақалада мемлекеттік органдар мен бизнестің бағдарламалық өнімдері арасындағы құпия ақпаратты біріктіруге, қауіпсіз және стандартталған деректер алмасуды қамтамасыз етуге арналған Smart Bridge платформасы талқыланады. Сыбайлас жемқорлыққа қарсы ақпараттық қауіпсіздіктің интеллектуалды жүйесі мен оқу жетістіктерін растау, сондай-ақ Қазақстан Республикасының жоғары оқу орындары мен әскери оқу орындарының студенттерінің, курсанттарының және түлектерінің ресми құжаттары мен ведомстволық ақпараттық жүйелер арасындағы деректерді біріктіру үшін электрондық үкімет шлюзімен өзара әрекеттесу архитектурасы әзірленді. Ұсынылған бағдарламалық модуль электрондық үкімет шлюзі арқылы жеке тұлғалардың мемлекеттік дерекқорынан жеке тұлғалар туралы ақпаратты алуға арналған. Өзара әрекеттесу деректердің шынайылығы мен тұтастығын қамтамасыз ету үшін электрондық цифрлық қолтаңбаны пайдаланып SOAP хабарлама форматында жүзеге асырылады.

Осылайша, Smart Bridge платформасын пайдаланып жүзеге асырылатын студент, курсант немесе магистратура порталында тіркелу кезінде электрондық цифрлық қолтаңбаны пайдаланып шақырылатын қызмет ұсынылады.

Түйінді сөздер: электрондық цифрлық қолтаңба, электрондық үкімет, SOAP хабарламасы, Smart Bridge, XML сұранысы.

Zhanna Yessengaliyeva, PhD, associate professor, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan

Olga Ussatova, PhD, associate professor, Institute of Information and Computational Technologies CS MSHE RK, Almaty, Kazakhstan

Sayat Zhumakhanov, master, Institute of Information and Computational Technologies CS MSHE RK, Almaty, Kazakhstan

DEVELOPMENT OF AN INTEGRATION SOFTWARE MODULE FOR ORGANIZING SECURE DATA EXCHANGE BETWEEN INFORMATION SYSTEMS

Abstract. This article discusses the Smart Bridge platform, which is designed to integrate confidential information between software products of government agencies and businesses, ensuring secure and standardized data exchange. To integrate data between an intelligent anti-corruption information security system and the validation of academic achievements, as well as official documents of students, cadets, and graduates of universities and military educational institutions

of the Republic of Kazakhstan, and departmental information systems, an architecture for interaction with the e-government bus was developed. The proposed software module is designed to retrieve information about individuals from the state database of individuals (GDPI) via the e-government gateway. Interaction is carried out in SOAP message format using an electronic digital signature to ensure the authenticity and integrity of the data.

Thus, a service called during registration on the student, cadet, or graduate portal using an electronic digital signature is proposed, implemented using the Smart Bridge platform.

Keywords: electronic digital signature, e-government, SOAP message, Smart Bridge, XML request.

Поступила: 04 января 2026 года
Рецензирована: 06 марта 2026 года
Принята: 12 марта 2026 год