BSecure DSS Lite – техническа спецификация

BSecure DSS Lite е Spring REST Web Service, който използвайки имплементирана Digital Signature Services библиотека на Европейския съюз, осигурява функционалности за създаване на електронно подписани документи в стандартизирани формати, съгласно Регламент 910/2014 (eIDAS). Освен това позволява удостоверяване на време на PDF документ, разширяване на форматите на електронно подписани документи, проверка на електронно подписани документи, както и освежаване на тези документи с цел дългосрочно съхранение. Поддържат следните формати с нива и тип на подписване:

Формати за електронни подписи

- CAdES (CMS Advanced Electronic Signatures) – формат, който изпълнява изискванията в европейски стандарт. Надгражда използвания до момента формат CMS/PKCS7 чрез смесването на подписани и неподписани атрибути, което позволява различни нива на подписване, чрез които да се постигне дългосрочно съхранение на подписаните документи. Форматът допуска електронно подписване на произволни файлове. Разширенията на подписаните файлове са познатите ".p7m" за тип на подписа “ENVELOPING” и ".p7s" за тип на подписа “DETACHED”.
- PAdES (PDF Advanced Electronic Signatures) - изпълнява изискванията на европейски стандарти и Надгражда използваният до момента PDF формат за електронно подписване (специфицирани в), чрез смесването на подписани и неподписани атрибути, позволявайки подпобно на формата CAdES да се постигне дългосрочно съхранение на подписаните PDF документи. Форматът допуска електронно подписване единствено на PDF файлове. За тип на подписа се поддържа единствено “ENVELOPED”. Разширението на файла след полагането на подписа е ".pdf".
- XAdES (XML Advanced Electronic Signatures) - изпълнява изискванията на европейски стандарти и Надграждат досегашния XML формат за полагане на електронен подпис чрез смесването на подписани и неподписани атрибути, което позволява дългосрочно съхранение на подписаните документи. Форматът допуска електронно подписване единствено на XML файлове. За типове на подписа се поддържат “ENVELOPED”, “ENVELOPING” и “DETACHED”. Разширението на подписан файл е ".xml".

Нива на подписване

- BASELINE_B – цифров подпис - базово ниво на електронния подпис. Осигурява цялост на подписания документ и неотменимост на положения електронен подпис.
- BASELINE_T – цифров подпис с Timestamp. Към базовото ниво на подпис е добавено удостоверено време (Time stamp) на подписване, като доказателство за съществуването на подписа към този момент.
- BASELINE_LT – цифров подпис с Timestamp и статус (OCSP/CRL). Към базовото ниво на подпис с удостоверено време (Time stamp), са добавени атрибути (CRL и OCSP), осигуряващи валидността на подписа, чрез проверка единствено на подписания файл, без да се изискват допълнителни проверки като статус на удостоверението за КЕП или търсене на сертификационната верига на удостоверението за КЕП. Целта на това ниво е да осигури информация за валидността на подписа при дългосрочно съхранение на подписания файл.
- BASELINE_LTA – цифров подпис с Timestamp, статус (OCSP/CRL) с възможност за валидиране след достатъчно дълъг период от време. Освен удостоверено време и допълнителни реквизити (Time stamp, CRL и OCSP) позволяващи самостоятелна проверка на подписа, позволява периодично актуализиране на удостовереното време и валидацията на подписа дълго време след създаването му. Целта на това ниво е да осигури цялост на информацията за валидността на подписа при достатъчно дълъг период на съхранение на подписания файл.

Тип на подписване

- ENVELOPED (Опакован подпис) - подписаният документ съдържа подписа, т.е. подписът е под елемент в подписания документ. Проложим към формати PAdES, XAdES.
- ENVELOPING (Опаковащ подпис) - подписът съдържа подписаният документ, т.е. целия подписван обект се намира в рамките на подписа. Приложим към формати CAdES, XAdES.
- DETACHED (Обособен подпис) - подписът и документа се намират в отделени файлове. Приложим към формати CAdES, XAdES.

BSecure DSSLite позволява интеграция с услуги за удостоверяване на време (Qualified TimeStamp), проверка за статус на електронен подпис (OCSP) и достъп до списъците с временно спрени и прекратени електронни подписи (CRL) за удостоверяване момента на подписване във времето, както и проверка валидността на удостоверението за електронен подпис. Услугите по Qualified TimeStamp, OCSP и CRL са услуги, неизменна част от инфраструктурата на Квалифицираните Доставчици на удостоверителни услугика.

BSecure DSSLite изгражда верига на доверие на удостоверенията за електронен подпис, съгласно европейският списък с квалифицирани доставчици на удостоверителни услуги (TSL – Trusted Service List), с което позволява използването на удостоверения за електронен подпис от всички такива европейски доставчици.

При работата си BSecure DSSLite осигурява възможности за :

- Изчисляване на данни за подписване на подаден документ (ToBeSign) според спецификациите на EU DSS библиотека;
- Изчисляване на данни за подписване при подаване на контролна сума и референция към външен файл със съдържанието за подписване (ToBeSign) според спецификациите на EU DSS библиотека;
- Създаване на подписан документ съгласно единните европейски формати за полагане на електронен подпис в синхрон с Регламент (ЕС) 910/2014 при подаване на външно изчислен цифров подпис;
- Създаване на подписан документ съгласно единните европейски формати за полагане на електронен подпис в синхрон с Регламент (ЕС) 910/2014 при подаване на външно изчислен цифров подпис (PKCS1) и референция към външен файл със съдържанието за подписване;
- Разширяване на ниво на подписване на подписан документ (BASELINE_B -> BASELINE_LTA, BASELINE_T -> BASELINE_LTA, BASELINE_LT -> BASELINE_LTA);
- Удостоверяване на време (Timestamp) на PDF документ;
- Проверка на електронно подписани документи (неквалифицирана услуга).

СТРУКТУРА

BSecure DSSLite се предоставя като spring boot jar файл, който се стартира и използва в инфраструктурата на клиента.

1. Параметри – конфигурират се през файлове application.properties и application-springboot.properties(намират се в bsecuredssl.jar>BOOT-INF>classes) и при предоставяне са със следните стойности по подразбиране:

    - application.properties:

        - spring.servlet.multipart.enabled=true – обработка на файлове

        - spring.servlet.multipart.max-file-size=10MB – максимална големина на файловете, които се изпращат към услугата

- spring.servlet.multipart.max-request-size=10MB – максимална големина на запитванията, които се изпращат към услугата
- tsa.service.timeout=10000 – timeout период (в милисекунди) за получаване на отговор от Timestamp сървър
- trusted.certs.file.name.classpath=classpath:TrustedCerts.jks – файл с доверени Root удостоверения на доставчици на удостоверителни услуги
- intermediate.certs.file.name.classpath=classpath:IntermediateCerts.jks – файл с доверени SubCA удостоверения на доставчици на удостоверителни услуги
- test.trusted.certs.file.name.classpath=classpath:B-TrustTestTrustedCerts.jks - – файл с доверени ТЕСТОВИ удостоверения на доставчици на удостоверителни услуги
- trusted.certs.keystore.password=1234 – парола за файл TrustedCerts.jks
- test.trusted.certs.keystore.password=1234 – парола за файл IntermediateCerts.jks
- intermediate.certs.keystore.password=1234 – парола за файл B-TrustTestTrustedCerts.jks
- tsl.lotl.url=https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-mp.xml - адрес на TSL списък с удостоверителни услуги според eIDAS. Изтеглените от списъка сертификати на Доставчици на удостоверителни услуги се записват във файл TrustedCerts.jks
- tsl.lotl.oj.uri=http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.C_.2016.233.01.0001.01.ENG - Information related to data on Member States' trusted lists
- tsl.delay=600000 – период/отлагане в милисекунди за изтегляне на TSL списък след първоначалното изтегляне при стартиране на приложението
- tsl.period=24 – период в часове на изтегляне на TSL списък (през колко часа да се обновява списъка)
- proxy.host, proxy.port, proxy.user, proxy.password – настройки за proxy за изходящ достъп към Интернет (в случай, че се използва proxy)

- Application-springboot.properties:

- tsa.service.address=http://tsa.b-trust.org – адрес на Timestamp сървър
- server.servlet.context-path=/bsecuredssl – контекст на приложението. В този случай приложението и неговите функции ще са видими на адрес: http://XXX.XXX.XXX.XXX:8080/bsecuredssl, а SWAGGER описание – на адрес: http://XXX.XXX.XXX.XXX:8080/bsecuredssl/swagger-ui.html, където XXX.XXX.XXX.XXX е IP адреса на сървъра, където е разположена услугата
- #server.port=8081 – по подразбиране приложението се стартира на порт 8080. Ако искате да промените този порт – премахнете коментара на реда(#) и укажете порт, на който да работи приложението
- proxy.host, proxy.port, proxy.user, proxy.password – настройки за proxy за изходящ достъп към Интернет (в случай, че се използва proxy)
- management.endpoints.enabled-by-default=false и management.endpoint.health.enabled=true стартират endpoint за health check на услугата (http://localhost:8080/bsecuredssl/actuator/health). Може да се види и в SWAGGER.

2. Логове – използва се стандартен log4j2. Параметри – във файл bsecuredssl.jar>BOOT-INF>classes>log4j2.xml. След стартиране на приложението ще се създаде поддиректория logs в директорията на bsecuredssl.jar.
3. Изисквания към инфраструктура
   - Java 8. За най-добра работа на приложението, следва да се използва последна версия на Java Server JRE.
   - Достъп до интернет (може и през proxy)
4. Swagger - BSecure DSSLite предоставя swagger описание на функциите със съответните параметри.
5. Health check (Actuator) - BSecure DSSLite предоставя възможност за изпращане на health check проверки за наличност на услугата.