**НОВ БЪЛГАРСКИ УНИВЕРСИТЕТ**

**БАКЪЛАВЪРСКИ ФАКУЛТЕТ**

**ДЕПАРТАМЕНТ "ИНФОРМАТИКА"**

**ПРОГРАМА** **ИНФОРМАТИКА**

**ДИПЛОМНА РАБОТА**

**ТЕМА: AS2 (Applicability Statement 2) сървър и клиент за трансфер на данни**

**НА СТУДЕНТА: Илиян Делчев Додеков ФАК. № 50129**

**НАУЧЕН РЪКОВОДИТЕЛ: Илиян Занкински**

**София**

**2015**

Съдържание

[Уводна част 3](#_Toc431948262)

[I. Резюме 3](#_Toc431948263)

[II. Мотивация 4](#_Toc431948264)

[III. Актуалност 5](#_Toc431948265)

[Използвана литература 6](#_Toc431948266)

# Уводна част

## Резюме

AS2 (Applicability Statement 2) е спецификация за това как да се трансферира информация сигурно и гарантирано в Интернет. Сигурността се постига с помощта на дигитални сертификати и криптиране.

AS2 е базиран на HTTP и S/MIME. Това е вторият AS протокол разработен и ползва същите конвенции за подписване, криптиране и MDN, както оригиналният AS1 от 90-те години. С други думи:

* Файловете са „закачени“ (attachment) към стандартизирано S/MIME съобщение (наричано още AS2 съобщение).
* AS2 съобщенията винаги се изпращат по HTTP или HTTPS протокол (Secure Sockets Layer не е задължителен) и обикновено с помощта на POST метод.
* Съобщенията могат да бъдат подписани с помощта на дигитален сертификат, но не е задължително.
* Съобщенията могат да бъдат криптирани с помощта на дигитален сертификат, но не е задължително.
* Съобщенията могат да поискат Message Disposition Notification (MDN), за потвърждение, че трансферът е успешен. Искането на MDN потвърждение не е задължително. MDN представлява съобщение, което следва нормите за трансфер на данни според AS2 протокола, но има специфично съдържание.
* Ако MDN потвърждение е поискано:
  + Когато дадено съобщение е получено, успешно декриптирано и подписа е верифициран, „успешен“ MDN ще бъде изпратен на изпращача на съобщението. MDN обикновено се подписват, но не се криптират.
  + Когато MDN съобщението бъде получено, декриптирано и подписа е верифициран, оригиналният изпращач ще знае, че трансферът е успешен (така наречената особеност – non-repudiation).
  + Ако има проблеми с трансфера може да бъде пратен „неуспешен“ MDN. Според протоколната спецификация обаче, липсата на MDN също означава „неуспех“.

Обикновено при AS2 трансфер има изискване двете страни, които обменят информация, предварително да си разменили набор от сертификати и идентификатори (т. нар. „имена на партньорите“). Имената на партньорите могат да бъдат всякаква валидна фраза.

AS2 спецификацията е описана подробно в RFC 4130 (Request for comment 4130). Дипломната работа ще имплементира стандарта до степен, в която следните функционалности са реализирани (както са описани в RFC 4130):

* HTTP транспорт
* S/MIME съдържание на съобщенията
* Криптиране с помощта на X509 дигитален сертификат
* Подписване с помощта на X509 дигитален сертификат
* Синхронен или асинхронен MDN

За осъществяването на успешен AS2 трансфер, софтуерът, който ще бъде изработен трябва едновременно да играе ролите на клиент и сървър (тоест изпращач и получател). За да се постигне това, ще се имплементира Java базирано решение.

За да се изпрати файл, разработеният продукт ще следи преконфигурирана директория за един или повече файлове и ще ги изпраща на даден получател посредством AS2. От друга страна, при получаване на съобщение, цялата информация ще бъде извлечена под формата на един или повече файлове и ще бъде записана в преконфигурирана директория.

Продуктът ще има възможност за проследяване на това как изглежда AS2 съобщението, когато се праща по мрежата. За да може да се демонстрира функционалността, продуктът ще бъде инсталиран два пъти, за да може двете инсталации да комуникират помежду си.

## Мотивация

Преди да взема решението за темата на дипломната работа, направих обстойно проучване какъв AS2 софтуер се предлага на пазара. Поради високата сигурност, сложност и изисквания на протокола, повечето решения таргетират ентърпрайз пазара, в резултат на което са доста скъпо платени. От друга страна решенията, които са безплатни и/или с отворен код са доста неразвити и неактуални. Повечето безплатни решения ползват доста стари технологии, в резултат на което имат неактуални имплементации. Също така се спират до реализацията на протоколната имплементация и нямат фокус на лесната работа с тях и имплементирането на функционалности, които да ги направят наистина използваеми в реалния живот.

Целта на тази дипломна работа е да се разработи AS2 комуникационен софтуер, който да покрива протоколната спецификация. Идеята е впоследствие да се подобри решението, така че да бъде възможно ползването му в реална клиентска среда. В същото време приложението ще бъде с отворен код.

## Актуалност

Въпреки че спецификацията е финализирана в RFC 4130 през Юли 2005 година, тя все още е актуална и всъщност е една от най-ползваните в световен мащаб. Това се дължи отново на факта, че протоколът се ползва предимно от ентърпрайз пазара за сигурен трансфер на данни – предимно EDI документи. Както знаем, промените в ентърпрайз пазара се внедряват доста бавно и като цяло, за да започне да се ползва дадена технология, тя трябва първо да се докаже. AS2 е добър пример за доказана технология.

От 2013 година се стандартизира и AS4 спецификацията, която до голяма степен спазва същите принципи за сигурност, но ползва SOAP протокол за транспорт и сигурност. AS4 като стандарт тепърва ще се доказва и ще навлиза в пазара. Неговата идея не е да замести AS2, а по-скоро дава възможност да бъде ползван от организации, които са искат да ползват или са инвестирали в web services(<http://www.drummondgroup.com/index.php/component/content/article/127-b2b/b2b-products/b2b-faqs/243-as4-faq> ).

# Използвана литература

<https://en.wikipedia.org/wiki/AS2>

<https://en.wikipedia.org/wiki/AS4>

<http://www.ld.com/as2-part-1-what-is-it/>

<http://www.ld.com/as2-part-2-best-practices/>

<http://www.drummondgroup.com/index.php/component/content/article/127-b2b/b2b-products/b2b-faqs/243-as4-faq>