From: Vladimir Dzhuvinov <vladimir@dzhuvinov.com>
Sent: 03/10/2016 21:21
To: DCIS
Subject: Коментари и предложения по еИД техническа спецификация

На вниманието на ДКИС:

Бих искал да отправя следните коментари и предложения относно качената за обсъждане спецификация за национална еИД система. Те са предимно в областта ЦЕИ / OpenID Connect / SAML.

1. Указване на OpenID Connect версия

В спецификацията не е указана версия на стандарта OpenID Connect, но той, както и SAML, разполага с версия - 1.0 [1].

2. OpenID Connect сертификация

Бих препоръчал изискване OpenID Connect ЦЕИ реализацията да премине сертифициране при OpenID фондацията, която се грижи за поддръжката на стандарта [2]. Това ще даде възможност да се провери дали и до каква степен реализацията съответства на стандарта и е съвместима със стандартен клиентски софтуер и библиотеки. Тестването се извършва автоматично чрез специален онлайн софтуер осигурен от OpenID фондацията, и може да се извършва многократно и още в процеса на разработка. За получаването на сертификат се дължи номинална такса.

3. Електронно подписване на автоматичните нотификации

Отн. т. 4.9 "Подсистема за автоматични нотификации при потребителски действия, събития и транзакции": За допълнителна защита нотификациите могат да се подписват от източника, и при възможност дори да се шифрират за съответния получател. В IETF започна работа по стандартен формат за това - Security Event Token (SET), виж [3].

4. Регистриране на наличните нива на потребителска автентикация

Бих препоръчал за ЦЕИ да се създаде [4] (и евентуално регистрира в IANA [5]) Level-of-Assurance (LoA) идентификатор и съответен профил за автентикацията с еИД (или повече, ако има различни нива на автентикация). LoA идентификаторите могат да се ползват както от SAML, така и от OpenID Connect за две цели: 1) дават възможност на клиента да укаже точно желаното ниво и метод на автентикация на потребителя; 2) сигнализира в издадените SAML assertions / ID tokens с какъв точно LoA е била сторена потребителската автентикация. Поддържането на LoA параметър също е от полза ако клиентите или свързаните услуги прилагат някаква

форма на федерация на идентичности.

5. Реализация на секторните идентификатори

Отн. т. 4.4.2.2 "Електронен идентификатор и секторни електронни идентификатори": Представеният пример за генериране на секторни идентификатори, който вероятно се базира на примера от OpenID Connect (OpenID Connect Core, т. 8.1) [6] се счита за технически недостатъчно безопасен, и вероятно ще бъде подменен с нарочна псевдослучайна функция (PRF), като HMAC-SHA256, в следваща ревизия на OpenID Connect спецификацията. Също така, AES примерът вероятно ще бъде подменен с AES SIV шифриране [7]. Вероятно с оглед на евентуални бъдещи изменения е най-добре да се укаже преглед на най-актуалните примери за секторен алгоритъм публикувани от OpenID.

6. Клиентска автентикация в OpenID Connect

Бих препоръчал автентикацията на самите софтуерни клиенти при OpenID Connect да бъде извършвана чрез метода private_key_jwt [8], особено за системно важни клиенти и услуги. Ползването на private_key_jwt дава редица предимства пред простите client_secret базирани методи, като възможност за ползване на HSM, защита на ключа при неволно изпращане на Token заявката по незащитен HTTP POST, и някои атаки описани в [10].

7. Допълнителни OpenID Connect защити

Също искам да обърна внимание на последните препоръки [9] на OpenID фондацията за защита на OpenID Connect реализации, в отговор на някои новооткрити атаки [10].

8. Общо предложение за добавяне на HMAC към сесийни, клиентски и прочие ключове / идентификатори

Бих препоръчал изпълнителят да разгледа целесъобразността за добавянето на допълнителна HMAC защита към издадени сесийни, клиентски и прочие идентификатори / ключове в OpenID Connect и на други места. Добавянето на HMAC би дало следните предимства: 1) ако идентификаторът е базиран на случайно число, евентуално компрометиране на системния генератор на случайни числа не би отслабило съществено случайността на крайния идентификатор; 2) намаляване експозицията към DoS атаки, които целят предизвикването на скъпоструваща операция, като заявка към база данни, използвайки невалидни идентификатори / ключове.

Успех!

Владимир Джувинов

[1] http://openid.net/specs/openid-connect-core-1_0.html

[2] http://openid.net/.../openid-connect-certification-program/

[3] https://tools.ietf.org/html/draft-hunt-idevent-token-05

[4] https://tools.ietf.org/html/rfc6711#section-1

[5] http://levelofassurance.org/registry.html

[6] http://openid.net/specs/openid-connect-core-1_0.html#PairwiseAlg

[7] https://tools.ietf.org/html/rfc5297

[8] http://openid.net/specs/openid-connect-core-1_0.html#ClientAuthentication

[9] http://openid.net/2016/07/16/preventing-mix-up-attacks-with-openid-connect/

[10] https://arxiv.org/pdf/1601.01229v3.pdf