Пулеко І. В., канд. техн. наук, доцент,
Топольницький П. П., канд. техн. наук, доцент,
Філіпов В. А., ст. викладач
Державний університет «Житомирська політехніка»

ОСОБЛИВОСТІ БЕЗПЕЧНОГО ПІДКЛЮЧЕННЯ ДАТЧИКІВ ІНТЕРНЕТУ РЕЧЕЙ ДО ХМАРНОГО СЕРЕДОВИЩА AZURE

Повсюдне впровадження систем Інтернету речей (англ.: Internet of Things, IoT) ставлять перед розробниками нові проблеми безпеки. Безпека IoT – це велика і серйозна тема, однак вона стає більш логічна і зрозуміла, ніж може здатися, у разі виконання конкретних проєктів з використанням послуг хмарних середовищ. Хмарні середовища, такі наприклад як Microsoft Azure, надають ряд переваг і можливостей щодо забезпечення безпеки пристроїв, що підключаються. Особливо помітні переваги при підключенні до хмари великої кількості однотипних пристроїв.

Нехай за умовами ведення бізнесу, потрібно підключити досить велику кількість (наприклад, декілька десятків) датчиків IoT до хмарного середовища Azure. Скористаємося для цього такими службами, як: Центр Інтернету речей Azure (англ.: Azure IoT Hub) та Служба підготовки пристроїв Інтернету речей (англ.: Device Provisioning Service, DPS)

Центр Інтернету речей Azure може управляти великими обсягами даних телеметрії, відправлених з багатьох датчиків. Кожен пристрій можна налаштувати окремо, щоб бути впевненим в його справжності. Проте при використанні багатьох пристроїв ця задача буде як мінімум обтяжлива. Процес перевірки автентичності пристрою називається «підготовка». Тому і необхідно застосовувати Службу підготовки пристроїв Інтернету речей (DPS), яка забезпечує майже автоматичну підготовку будь-якого числа пристроїв.

Тоді сценарій безпечного підключення датчиків IoT до хмари можна подати у вигляді наступних кроків:

Крок 1. Створення ресурсу користувальницького Центру Інтернету речей Azure.

Крок 2. Підготовка пристроїв до сертифікації X.509 і реєстрації.

В основі сертифікатів X.509 лежить концепція шифрування з відкритим і закритим ключами. При використанні цієї сертифікації зі службою підготовки пристроїв Azure (DPS) інфраструктура відкритих ключів вбудована в службу, що значно спрощує роботу.

Служба підготовки пристроїв Azure може бути пов’язана з одним центром Інтернету речей або декількома і може розглядатися як система управління сертифікатами та реєстрацією.

Крок 3. Створення Служби підготовки пристроїв, кореневого сертифіката і групової реєстрації. DPS може бути пов’язана з одним центром або декількома. Тобто, це окремий ресурс, який не залежить від конкретного Центру Інтернету речей. Ресурс DPS створюється так само, як і будь-який інший ресурс Azure. Як політику доступу доцільно обирати iothubowner.

Крок 4. Створення кореневого сертифіката X.509 за допомогою Служби підготовки пристроїв. Перш ніж цей сертифікат ЦС можна буде використовувати для перевірки справжності пристроїв в DPS, необхідно провести Підтвердження належності сертифіката.

Крок 5. Підтвердження належності сертифіката ЦС надається службі DPS шляхом відправки сертифіката перевірки, створеного на основі кореневого сертифіката. Сертифікат перевірки містить створений код перевірки. Всі ці сертифікати будуть самозаверяємі.

Крок 6. Створення групової реєстрації в службі DPS в Azure. На цьому кроці створюємо один кінцевий сертифікат для кожного пристрою, дані телеметрії з якого планується відправляти в центр.

Крок 7. Створення коду для пристроїв датчиків. Обиравши інтегроване середовище розробки (IDE) свого додатку та створюємо код, що виконується на кожному пристрої датчика. Одна з цілей полягає в тому, щоб зробити код для кожного пристрою максимально ідентичним і тим самим звести до мінімуму участь людини. Для коду потрібно одне коригування при підготовці для другого пристрою: шлях до кінцевого сертифікату повинен бути унікальним для кожного пристрою. Унікальність цього випадку означає зміну «1» на «2» або «3».

Крок 8. Тестування автоматичної підготовки та призначення в Центр для декількох пристроїв. На цьому кроці перевіряється, чи працюють всі датчики належним чином. Спочатку ми перевіряємо, чи отримує центр Інтернету речей автоматично оновлення зі списку підключених пристроїв IoT. Далі ми перевіряємо, чи отримує центр дані телеметрії з пристроїв. Потім, на порталі змінюємо параметр двійника для одного пристрою і переконаємося, що зміни приходять на потрібний пристрій.

Таким чином, ми застосували технології зіставлення кореневого і кінцевих сертифікатів X.509 з центром Інтернету речей і пристроями IoT в ньому; створили кореневі і кінцеві сертифікати X.509; створили додаток для відправки телеметрії пристрою в центр Інтернету речей за допомогою Visual Studio Code; протестували кілька пристроїв IoT, підготовлених ресурсом DPS.