IoT CERTIFICATES REGISTRATION FOR CLOUD PROVIDERS

INVENTOR:

MASSIMILIANO PALA

Description

A non-obvious method to allow the registration of IoT certificates for cloud providers. The idea reverts the approach originally envisioned by the cloud providers (e.g., AWS) and does the following:

- The Certificate Service Provider opens an IoT Account
- The Certificate Service Provider registers one or more SubCAs that it uses to issue certificates for its customers by providing, for each of them, the required CA authentication token
- The Certificate Service Provider uploads / registers the certificates it issued for the customer's IoT Devices to its own IoT account (i.e., by registering each issued certificate separately, by registering the certificates in batches, or via any other specific methods provided by the cloud provider)
- The Certificate Service Provider gets permission by the customer (e.g., via API keys, authentication tokens, or other method) to move the registered IoT Device certificates to the customer's account together with a customer's indicated policy for each certificate (this enables the use of the certificate in such a way that when the device connects to the cloud IoT service they directly connect to the customer's device)

This method allows the Certificate Service Provider to securely register the certificates and enable them for usage under the customer's account without exposing the SubCA's authentication token in the customer's account directly.

Problem You’re Solving?

Cloud providers (AWS) require that IoT device certificates are pre-registered in order for the device to be associated with a customer's account. The current registration process implies the use of a SubCA specific for each account. The registration process requires the customer to provide an authentication token (e.g., a certificate with a special authentication token in it) that must be issued by the CA that issued the IoT devices' certificates. This makes it impossible for Certificate Service Providers (or CSPs) to provide automated device certificates' registration service on their customers' behalf (customers = the entity that requested the certificates' devices) without security concerns (i.e., without allowing the customer to register certificates issued under that CA not purchased or issued to that entity).

Our process allows Certificate Service Providers (or CAs) to pre-register the issued certificates securely and then transfer the ownership of the specific customer without exposing the authentication token within the customer's cloud account - thus removing the security concerns (from the CSP/CA perspective) during the registration process.

Why CableLabs?

CableLabs is heavily involved in the IoT space with several projects. In particular, the Diablo project is aimed at providing a fully integrated solution for IoT credentials deployment and cloud integration. The current target is AWS, but the process might be extended to other cloud providers if they provide similar features.

Hypothesis and Supporting Assertions

The current registration process within AWS is the following:

- The customer opens an AWS IOT account
- The customer registers a SubCA together with the authentication Token
- The customer uploads the IoT certificates individually or via Batch APIs (or via a just-in-time registration which basically allows any certificate issued under the registered SubCA to be allocated to the customer's account)
- The customer associates (if not already done at upload/auto-registration step) a policy to each certificate

Automated IoT Credentials Integration with Cloud Providers

A novel process for Credentials Providers to provide full integration with Cloud services

Inventor: Massimiliano Pala

Three Entities

- **The Certificate Services Provider.** This entity is the one that issues the certificates for its customers
  - The CSP is the entity that registers the issued credentials with the cloud provider on behalf of its customer
- **The Cloud Provider.** This entity provides the cloud-based services and requires the IoTs to be authenticated via a valid X.509 certificate
- **The Client.** This entity is the one that requested or bought the certificates from the CSP and also wants the IoT credentials (the issued certificates) to be automatically registered with the cloud provider under its own (the client) account

Description

- Cloud providers (e.g., AWS) require that IoT device certificates are pre-registered in order for the device to be associated with a customer's account.
- The current registration process implies the use of a SubCA specific for each account
  - The registration process requires the customer to provide an authentication token (e.g., a certificate with a special authentication token in it) that must be issued by the CA that issued the IoT credentials
  - The token allows to register any certificate issued by that CA under the account where the CA token is registered

Description (cont.)

- This makes it impossible for Certificate Service Providers (or CSPs) to provide automated IoT credentials registration service on their customers' behalf without security concerns
  - Registering a token related to a CA that issues certificates for different customers might allow one client to register devices that she does not own just because they were issued by the same CA

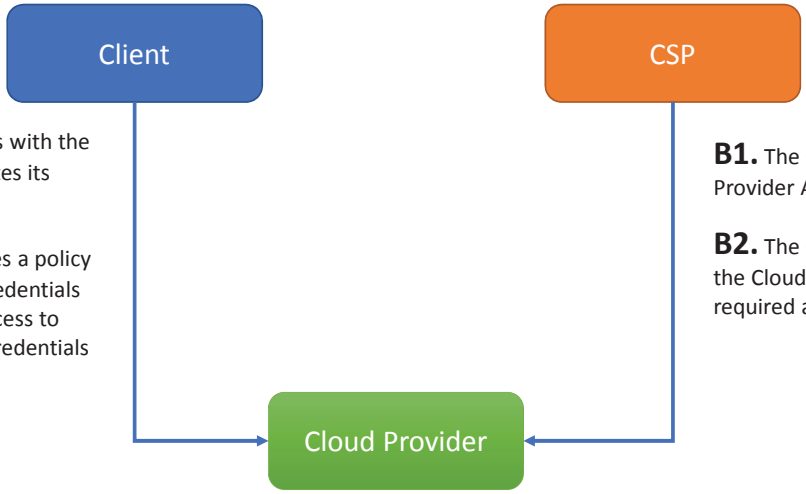
What Does Our Solution Provide ?

- Our process allows Certificate Service Providers (or CAs) to use the same CA for different customers by not requiring the client to demonstrate ownership over the issuing CA during the registration process of certificates

The Process in a Nutshell

- Our solution turns the registration process upside down in that it separates the registration of the IoT credentials from the enabling of their usage within the client's account
- In a Nutshell the Process can be summarized as follows
  - The issuing CA's authentication token is properly registered with the CSP's cloud account (this provides the possibility to register all credentials issued by that CA under the CSP's cloud account)
  - The CSP registers the issued Credentials (certificates) the cloud provider under the CSP's account (instead of the client's one)
  - The Credentials (certificates) issued for a specific client are transferred to the client's cloud account
    - This does not require the registration of the CA's authentication token under the client's account thus allowing the use of a single CA for different clients

Pre-Requisites



A1. The Client Registers with the Cloud Provider and creates its Own cloud account

A2. The Client generates a policy to be used during the credentials (certificate) transfer process to activate the use of the credentials

B1. The CSP registers with the Cloud Provider And creates its own account

B2. The CSP registers the issuing CA with the Cloud Provider by generating the required authentication token

The Process Flow

P1 The Client Requests the credentials for its own IoT devices and provides the required credentials (e.g., an API key) to allow for the issued certificates to be transferred to its own (the Client's) cloud account

P1.b (optionally) The client provides additional metadata (e.g., a policy or a reference to a policy) to use during the IoT credentials' transfer from the CSP's cloud account to the Client's one

P2 The CSP registers the issued certificates with the cloud provider under its own account

P3 The CSP transfers the registered credentials from its own account to the Client's one without registering the CA's authentication token in the Client's account by using the provided credentials (e.g., the API key) and metadata (e.g., a policy or a reference to a policy, etc.)

P4 The IoT can now connect securely by using the registered device credentials