A notification system over the HTTP protocol for web services

@fjmtu

2021 11/17

Background & Motivation

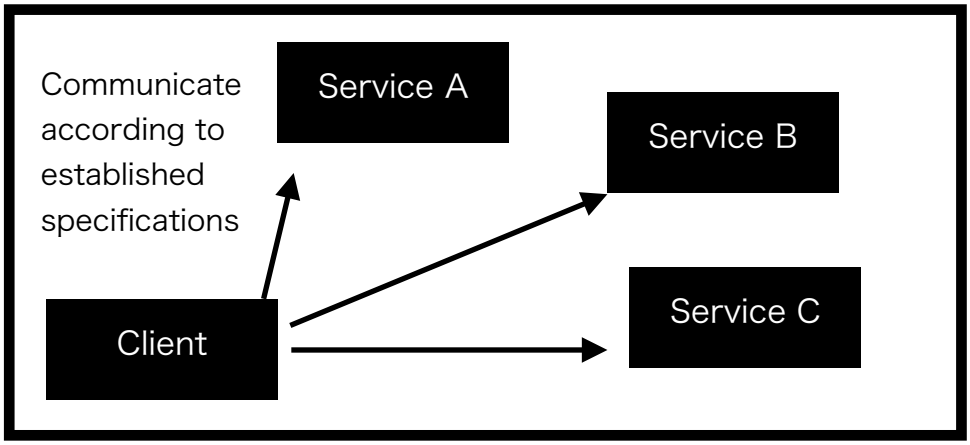
In today's web services, notifications to users are generally delivered by e-mail. However, delivering notifications via email involves the following problems.

1. When your email address changes, you need to change it for all the services you have registered with.
2. The service will know your email address (which is not good for people who value their privacy)
3. The content is known to the email service provider because there is no E2EE

Therefore, I would like to solve these problems by connecting web services and users directly.

Procedures

Overview



Basic steps

1. The token for authentication when retrieving notification content is determined between the service and the client. The service also tells the client the endpoint information for retrieving the notification content.
2. When the client wants to retrieve the notification, it sends an HTTPS request to the endpoint received from the service with the HTTP header "NOTIFY-TOKEN=token" (do not use HTTP).

3. Upon receiving the request, the service will authenticate the client. If the authentication is successfully completed, the service will deliver a notification with the following data structure.

```
{
    "body": [
        {
            "id": "UNIQUE ID",
            "title": "MESSAGE TITLE",
            "body": "MESSAGE BODY",
            "sent-date": "TIMESTAMP",
            "delete-date": “TIMESTAMP or NONE”
        }
    ]
}
```

Reissue token

If the token is compromised, the user will login to the web service and follow the procedure for reissuing the token.

Control of token

Users need to manage a token for each service. Such a hassle can be avoided with a bit of software ingenuity. For example, when the token transfer button is pressed, the token information and service information stored in the file can be paired and imported.