



 **zammo.ai**

Security



In This Presentation

- Multi-factor authentication
- Data analytics & analytics API
- Data collection
 - Push of information
 - Pull of information
- PII information in data analytics
- Using authentication to protect customer data
- SSL reports

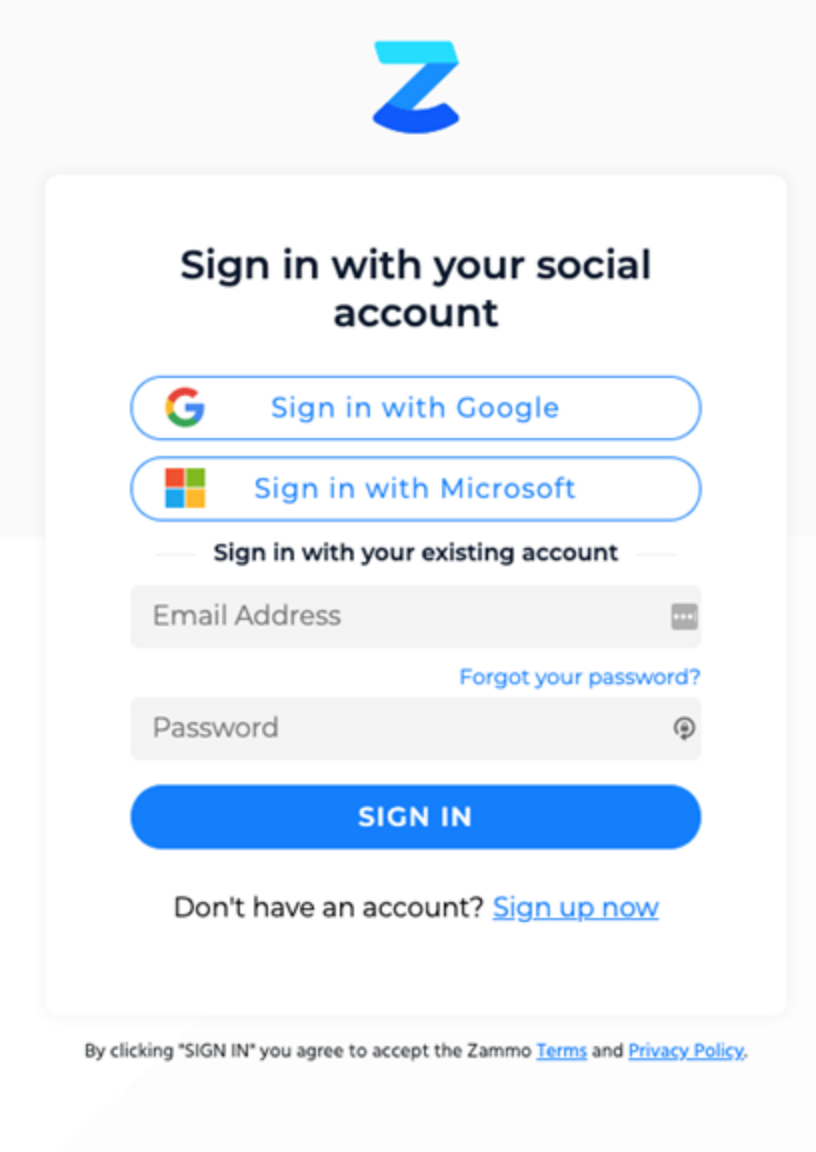


Using MFA to Login to Zammo

For security purposes, many organizations require multi-factor authentication for any online services.

When your team creates their account or signs in to Zammo, they have the option to sign in with either Google or Microsoft.

When one of those options is selected, Zammo delegates the authentication to that service, therefore providing the security of multi-factor authentication provided by Google or Microsoft.



The screenshot displays the Zammo login interface. At the top center is the Zammo logo, a stylized 'Z' in blue and cyan. Below the logo, the heading reads "Sign in with your social account". There are two prominent buttons: "Sign in with Google" (with the Google logo) and "Sign in with Microsoft" (with the Microsoft logo). Below these is a link for "Sign in with your existing account". The form includes an "Email Address" input field with a visibility toggle, a "Forgot your password?" link, and a "Password" input field with a visibility toggle. A large blue "SIGN IN" button is positioned below the password field. At the bottom of the form, there is a link: "Don't have an account? [Sign up now](#)". At the very bottom of the page, a small disclaimer states: "By clicking 'SIGN IN' you agree to accept the Zammo [Terms](#) and [Privacy Policy](#)."



Data Analytics & Analytics API



What Data is Collected?

- Engagement data collected includes:
 - Platform used (Google, Alexa, chatbot, Telephony)
 - Timestamp
 - Word-for-word question user asked
 - Answer the bot provides in response
- No PII information is collected or stored (i.e. user name, location, IP address, etc.)
- If your workflow requires PII to be collected, reference slide 11 for options and layers of protection.



“What are your hours of operation?”



“We are open from 9 to 5.”

This data can be consumed two ways:

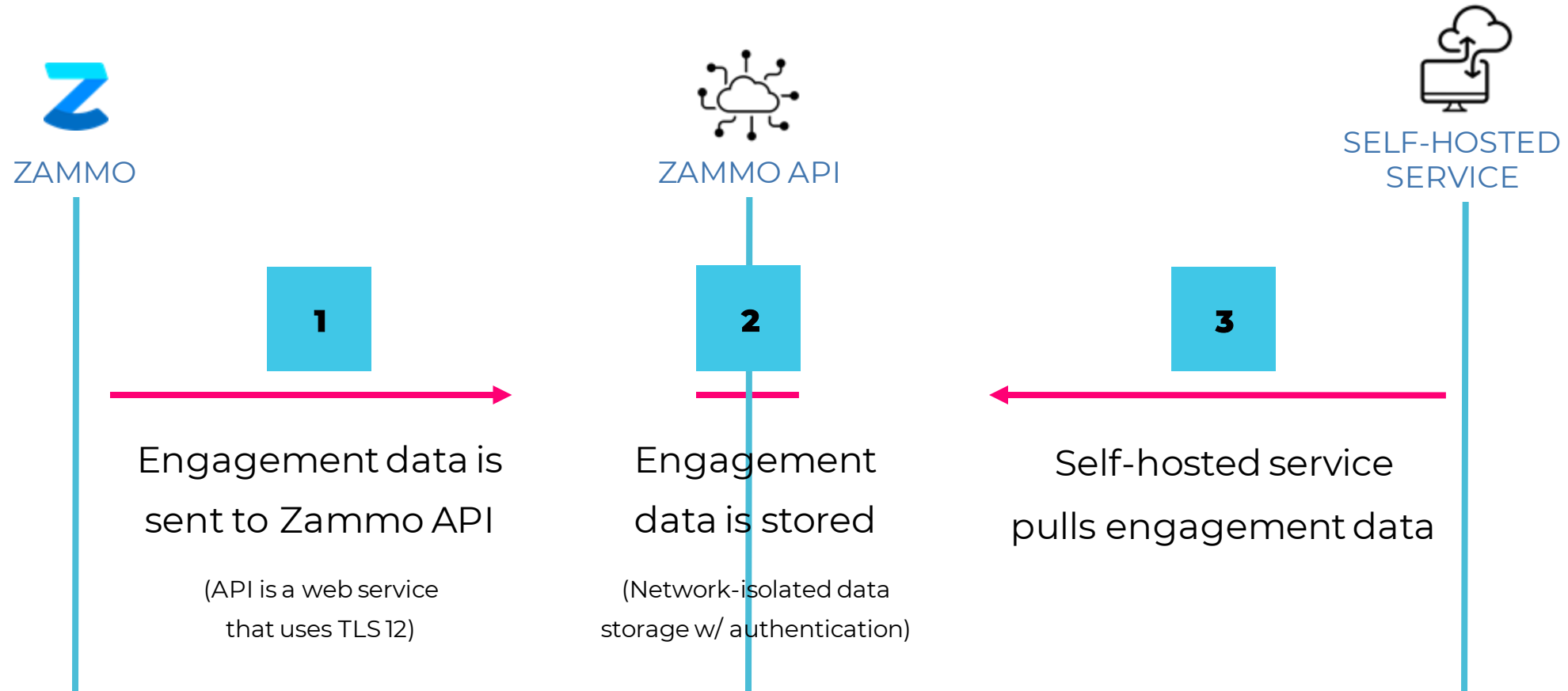
- Through the Zammo portal, you can view consolidated analytics and download raw data in a spreadsheet.
- Using Zammo’s analytics API, data can be pulled or pushed to a self-hosted service.



Data Pull to Self-Hosted Service

Engagement data **"pull"** is the **default** option to get data to a self-hosted data store.

Customers can pull engagement data using the Zammo API with authentication. This pull can be done as often as needed.

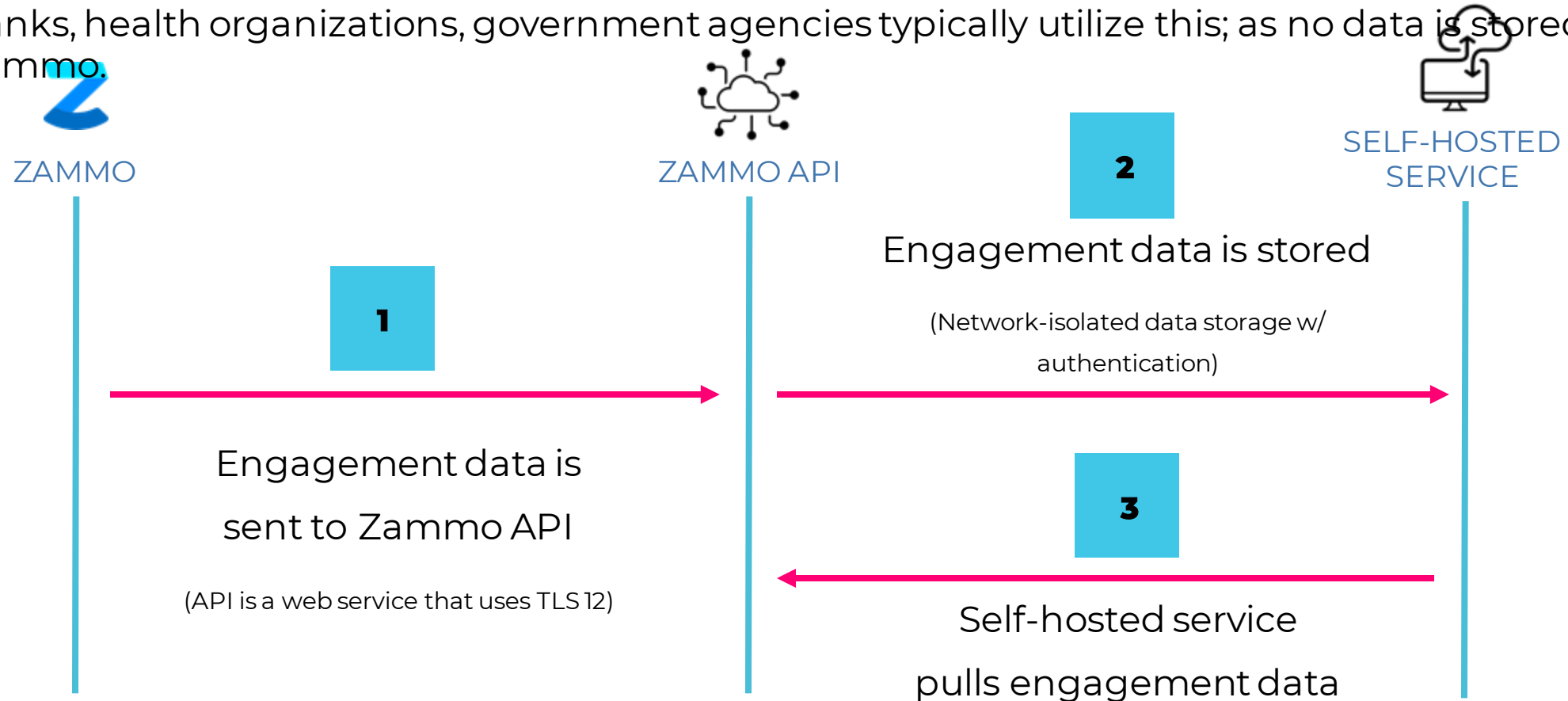


Data Push to Self-Hosted Service

To avoid Zammo storing any information, Zammo also offers connecting to an API (with authentication) exposed by the customer (ie web hook), to which Zammo can **push** the user engagement data.

The customer API would control delivery acknowledgment and throughput.

Banks, health organizations, government agencies typically utilize this; as no data is stored with Zammo.



PII Information in Data Analytics



Zammo Offers Two Main Layers of Protection for PII

BEFORE (To prevent PII from getting in the analytics spreadsheet)

- Content moderation – The data is obfuscated. Personal data such as email address, IP address, U.S. mailing address, SSN, and U.S. phone number can be filtered. The filter can be turned on specifically for the customer use case, and users are only able to see stars in the analytics transcript. This feature is not turned on by default as there may be instances where a customer will need to collect data (such as email addresses) for specific reasons.
- The customer can choose to turn off analytics altogether to prevent any data from being logged.

AFTER (Once data has been included in the analytics spreadsheet)

- The data is stored in a SQL server in the Microsoft Azure Cloud that includes:
 - Firewall Access – Only individuals with a specific IP address can have access to the database.
 - Strong Password – Only specific authorized users have access to the system. At the database level, a user role needs to be authorized prior to access. The user must not only have the password, they need to have their specific network IP address authorized prior to access.



Using Authentication to Protect Customer Data



Workflow Requires User Logging In To Get Personal Data

- When authentication is required in a workflow, the platform will redirect the user to your service's authorization endpoint.
- User signs in and grants your voice app / chatbot permission to access their personal data.
- A token is sent to Zammo, allowing the dialogue to continue. Zammo does not store anything and only has interactions with that particular service.
- Authorization endpoint hosts the mapping between OAuth token and the user's actual identity on Google/Alexa/Microsoft.
- See diagram on next slide.
- Platform specific diagrams can be found at these links:
 - [Google](#)
 - [Alexa](#)
 - [Microsoft](#)



Workflow Requires User Logging In to Get Personal Data



PLATFORM



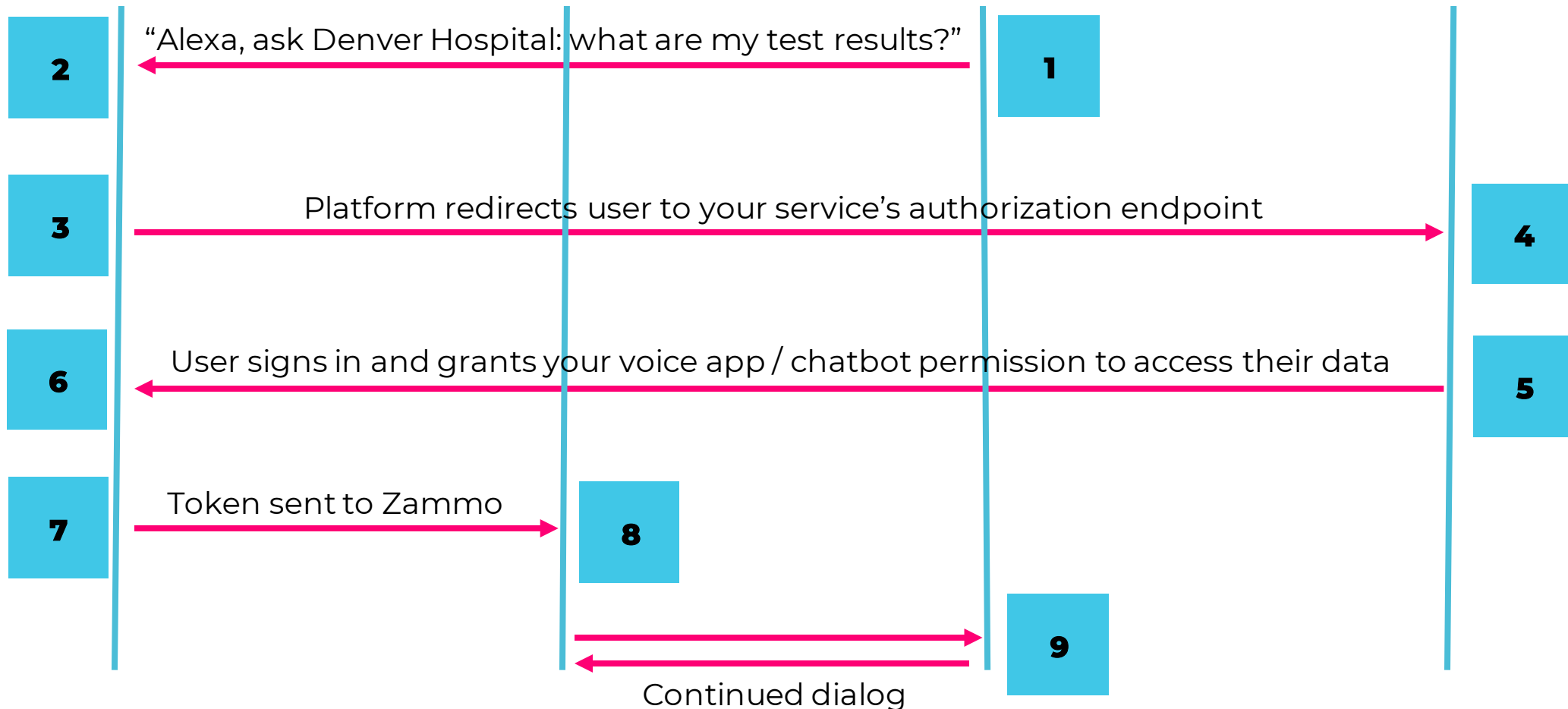
ZAMMO



USING A VOICE ASSISTANT



AUTHORIZATION SERVER/
ENDPOINT



SSL Reports

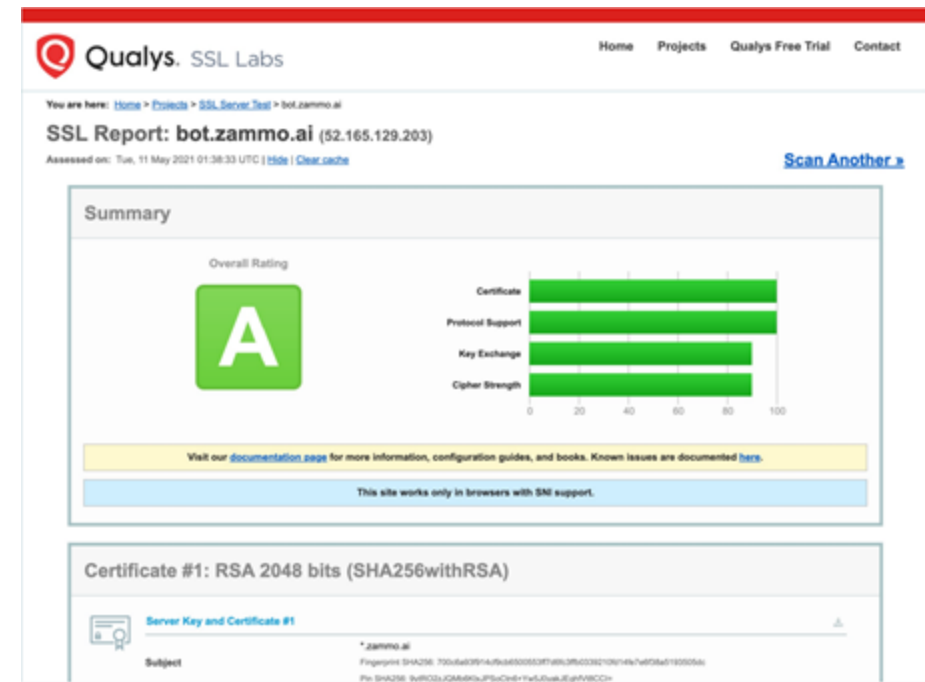
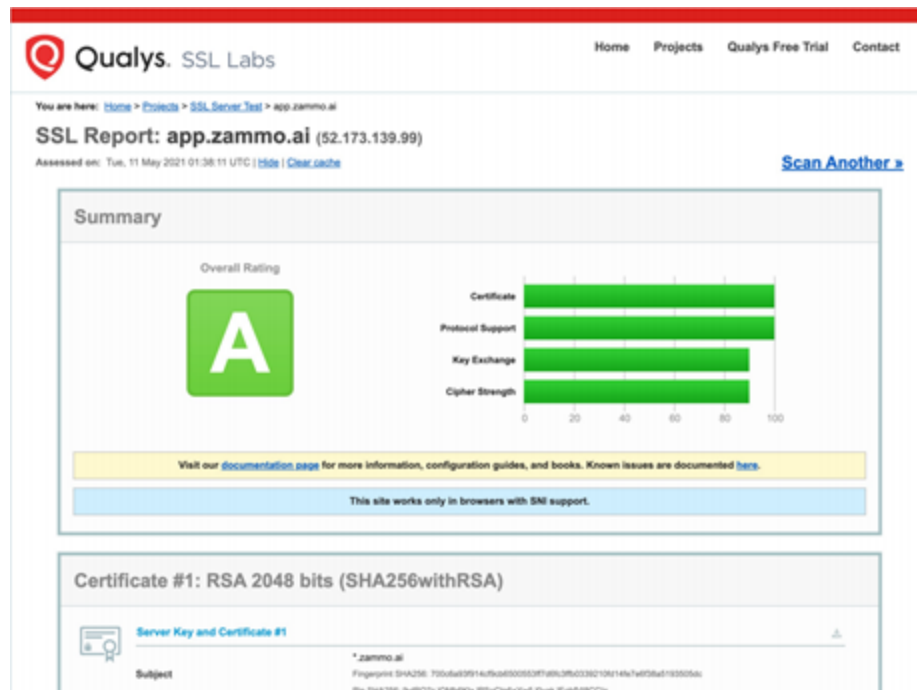


Services

The ZammoBot and API are two web services accessible through **app.zammo.ai** and **bot.zammo.ai**.

The SSL analysis reports below show an evaluation of the infrastructure for the two services.

That evaluation below does not include a review of the additional authentication mechanism that ensures a second layer of security for data manipulation.



Services

Zammo uses Direct Line API 3.0 with all of the recommended security guidance listed [on this page](#) implemented.

The communication also transits through Azure Bot Service, which itself has a full description of its security guidelines for the data in transit and at rest accessible [on this page](#).

API 3.0





Thank You

