Blaise Security Improvements

Statistics Netherlands - Robert Beisicht

2016 BLAISE
17TH INTERNATIONAL BLAISE USERS CONFERENCE

Token Based Authentication & Authorization

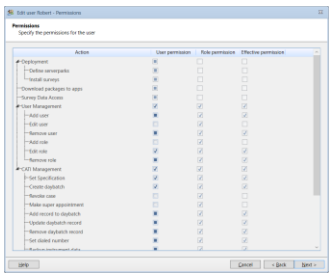
- Users authenticate themselves with the Security Token Service (STS).
- The STS issues a signed token that contains all permissions.
- The token is protected from manipulation with strong cryptography.
- The token is sent along with all calls to the services.
- Services can verify whether the token originates from our STS.

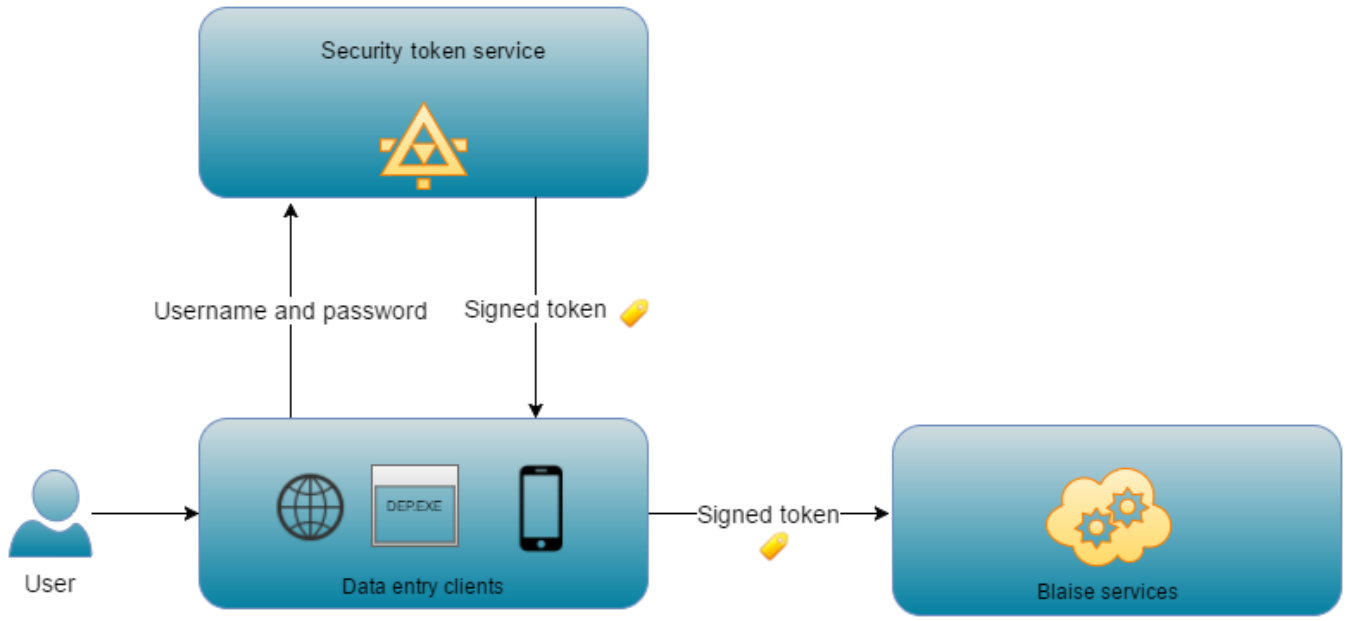
Fine-grained access control

Permissions are specified in the Server Manager and can be defined on two levels:

- Role permissions
- User permissions

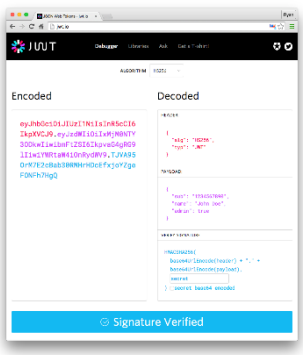
A role can be assigned to a user, giving him/her all the permissions that that role has. Permissions can be overridden for a particular user.





JSON Web Tokens (JWT)

Tokens are digitally signed to prevent tampering and its format relies on an open industry standard (RFC 7519).



Transport Layer Security (TLS)

In addition to token based authentication, all client applications can be configured to use Transport Layer Security. This protocol is best known for its use on websites which have an address that starts with *https://*, indicating that the browser should use TLS for the connection.

TLS is designed to prevent eavesdropping of sensitive information by using strong data encryption for the whole communication process. When using a server certificate with TLS, the client is also able to verify the authenticity of the Blaise service endpoints.

BLAISE by Statistics Netherlands
SURVEY SOFTWARE FOR PROFESSIONALS