B3i | COMMUNITY

Authentication & Authorisation

INTERVIEW

B3i's Ken Marke, recently sat down with Philipp Tölle, one of B3i's Solutions Architects, to gather insight on the topic of Authentication and Authorisation in a distributed environment. To explore the unique challenges the team have overcome and how they are making best use of current technology at B3i.

Philipp Tölle is currently responsible for driving forward the B3i network vision and actively building bridges with our customers to support their adoption and implementation of Distributed Ledger Technology.

VIDEO INTERVIEW

Authentication and Authorisation in a Distributed Environment

Watch the full interview here:
https://youtu.be/XRqr1s9cetg

Authentication & Authorisation

Authentication or Authorisation

When we talk about authentication, we are simply asking 'who are you' – whilst authorisation is establishing 'what are you allowed to do'.

Tölle describes this simply by saying, "Authentication is the answer to the question who are you and authorisation is the question what are you allowed to do, so they're usually used in the same context but they essentially two separate things because they are two separate answers to two different questions."

In the context of B3i, who is building a distributed enterprise system – for more than just one client – that needs to implement a mechanism that is capable of identifying many different parties looking to access the platform.

Implementation

Relying on open standards is the best way to tackle the challenges posed by the inherent complexity of different organisations, internal organisations structures and Identity Management solutions, and their interaction with one platform.

B3i specifically chose to adopt the 'JSON Web Token (JWT) Standard' as the data carrier to quickly and securely transmit the information required for authentication and authorisation on the B3i platform.

In a Reinsurance agreement scenario, this ensures B3i has the answer to who is requesting access to the platform (authentication), and secondly establish the permissions allowed to create a Reinsurance agreement (authorisation) on behalf of the customer's company in the node that is deployed at the customer's data centre.

JSON WEB TOKEN (JWT)

An open standard (RFC 7519) that defines a compact and self-contained way for securely transmitting information between parties as a JSON object. This information can be verified and trusted because it is digitally signed. JWTs can be signed using a secret (with the HMAC algorithm) or a public/private key pair using RSA or ECDSA.

AUTHORISATION

This is the most common scenario for using JWT. Once the user is logged in, each subsequent request will include the JWT, allowing the user to access routes, services, and resources that are permitted with that token. Single Sign On is a feature that widely uses JWT nowadays, because of its small overhead and its ability to be easily used across different domains.

INFORMATION EXCHANGE

JSON Web Tokens are a good way of securely transmitting information between parties. Because JWTs can be signed—for example, using public/private key pairs—you can be sure the senders are who they say they are. Additionally, as the signature is calculated using the header and the payload, you can also verify that the content hasn't been tampered with.

Authentication

& Authorisation

Authentication in a Distributed Environment

In a Distributed Environment, the same software needs to be distributed across the network. For the purposes of authentication, we simplify the process by removing client specific requirements. Employing one open interface, the JWT standard, where the authentication 'token' is supplied in a specific way by everyone.

Our platform then authenticates that the token has been produced by the correct company and as expected by our rules. Cryptography ensures this is done securely, allowing (authorising) the party to create and capture the necessary information on their record.

B3i provides a clear interface for the individual customers and what information the token needs to contain, following the Open ID Connect (OIDC) standard. B3i has also standardised the conversation – *"how you get the token and how you push the token into the system, by utilising the Implicit Grant Flow."*

Challenges of Authorisation

Tölle explains in a scenario, the challenges of authorisation effectively try to establish:

"Is an Underwriter allowed to just by himself sign the treaty above 20 million dollars?"

Quick to answer his own question, Tölle tells us that this rule would be established by the regulator, given to the Reinsurance company, outside of the B3i platform. Something specific to a region, the company, and legal environment of the business.

B3i provides a clear interface which is configurable by the customer. It's the token (authorisation) then which dictates whether that user has the appropriate privileges, and if those actions are permitted or disallowed if they don't fit the agreed limits.

Authentication & Authorisation

Summary

Put simply, Authorisation is not the same as Authentication.

In a distributed environment like B3i's network, authentication quickly establishes who you are using the well-established JSON Web Token Standard (JWT).

However, authorisation enables you to set rules around what authorised users can actually do. This is critical for Insurance and Reinsurance businesses who need to exercise control and set privileges across their node in line with Regulatory requirements and internal business requirements and compliance needs. A good example is establishing controls for Underwriters.

B3i ensures that customers are who they say they are, can enact changes to their data safely across the network and within the limits set out by the customer.

Philipp Tölle

Philipp Tölle is a Solutions Architect with B3i, seconded from Swiss Re.

Philipp is part of the core development team, which created the well acknowledged B3i Proof of Concept (launched 2017 Monte Carlo).

He has been working with the team to drive forward the B3i Network Vision and actively building bridges into the IT organisations for Swiss Re and other B3i customers.

Prior to his involvement with B3i and the Swiss Re Blockchain activities, Philipp has been responsible for the data integration part of the renewed group wide financial planning landscape in Swiss Re.