June 2023

PASSPORT IMMIGRATION CONTROL FOR DIGITAL CITIZENS TRAVELLING BETWEEN METAVERSES

Ishita Maheshkumar Thanki

Amanda L Holst

Ana Montenegro

David Hanes

Sudha Katgeri

PASSPORT IMMIGRATION CONTROL FOR DIGITAL CITIZENS TRAVELLING BETWEEN METAVERSES

AUTHORS:
Ishita Maheshkumar Thanki
Amanda L Holst
Ana Montenegro
David Hanes
Sudha Katgeri

ABSTRACT

In a metaverse, the online digital manifestation of a user is commonly referred to as a digital citizen. Such a digital citizen is most often represented by an avatar and its associated metadata. Currently, a digital citizen is isolated to their own metaverse and a new avatar and/or metadata must be created when the digital citizen wishes to enter a new metaverse. Techniques are presented herein that support a checkpoint for digital citizens that are traveling from one metaverse to another and that serve as a verification system on a centralized or distributed server. The presented passport immigration control framework allows digital citizens to travel to other metaverses outside their metaverse of origin, while protecting the rights of users as digital citizens. Such controls establish and strengthen mechanisms to monitor the impact of future liabilities, legislative enactments, and user accountability. The presented framework also provides guidelines for the best standards that entities may take while assessing identity and tracking for a digital citizen. Use of the presented techniques can safeguard protections for digital citizens in a metaverse and encourage an entity's customers to invest in business and benefit by adopting the presented framework.

DETAILED DESCRIPTION

In a metaverse, the online digital manifestation of a user is commonly referred to as a digital citizen. Such a digital citizen is most often represented by an avatar and its associated metadata.

Currently, a digital citizen is isolated to their own metaverse and a new avatar and/or metadata must be created when the digital citizen wishes to enter a new metaverse.

Published by Technical Disclosure Commons, 2023

Each metaverse has its own unique features, capabilities, and requirements for its digital citizens. As the different metaverses evolve, digital citizens will want to travel across metaverses and carry their avatars and metadata with them.

However, there are no standards that define how such travel will be made possible while ensuring security for both the metaverses and a digital citizen.

A number of existing solutions attempt to address different aspects of the challenge that was described above. A first offering supports a framework for creating and managing a non-fungible token (NFT) identity on a blockchain network through a self-sovereign identity (SSI) model. A user of that offering may bond their identities to their digital and physical assets. The techniques presented herein (which will be described and illustrated below) are complimentary to that offering, in that they provide another way to verify that a digital citizen is in fact a digital citizen. The presented techniques offer a passport control facility for digital citizens that are travelling between metaverses and, consequently, those techniques may leverage the first offering if it is employed by a digital citizen.

A second offering is touted as a connective passport for the metaverse – i.e., it is a technology that provides consumers with a universal avatar that they can use not only in one world but also in many virtual platforms. The techniques presented herein are complimentary to that offering. If a user has an avatar in the second offering, the presented techniques can leverage that avatar for travel to another metaverse. The second offering ensures that a universal avatar can meet certain requirements such as a minimum degree of resolution. The passport immigration concept under the techniques presented herein ensure that a compatible avatar from the second offering is used when traveling while also ensuring that the necessary metadata for entry and a visa is included.

A third offering provides a baseline set of standards, guidelines, and best practices for a metaverse. However, as noted above, there are no ratified standards for travelling across metaverses. The techniques presented herein support a framework that can be adopted by the different standards bodies, if they so choose.

To address the challenge that was described above, techniques are presented herein that support a passport and immigration framework that enables secure travel across metaverses.

If a user wishes to just remain in their own metaverse, then the techniques presented herein do not apply. However, if they wish to travel to another metaverse using the same avatar and metadata, they may, according to the presented techniques, apply for a passport where more personal information may need to be submitted.

The techniques presented herein may be explicated through an illustrative example. Under that example, a digital citizen wishes to travel from one metaverse (such as Metaverse 1) to another metaverse (such as Metaverse N), as depicted in Figure 1, below.

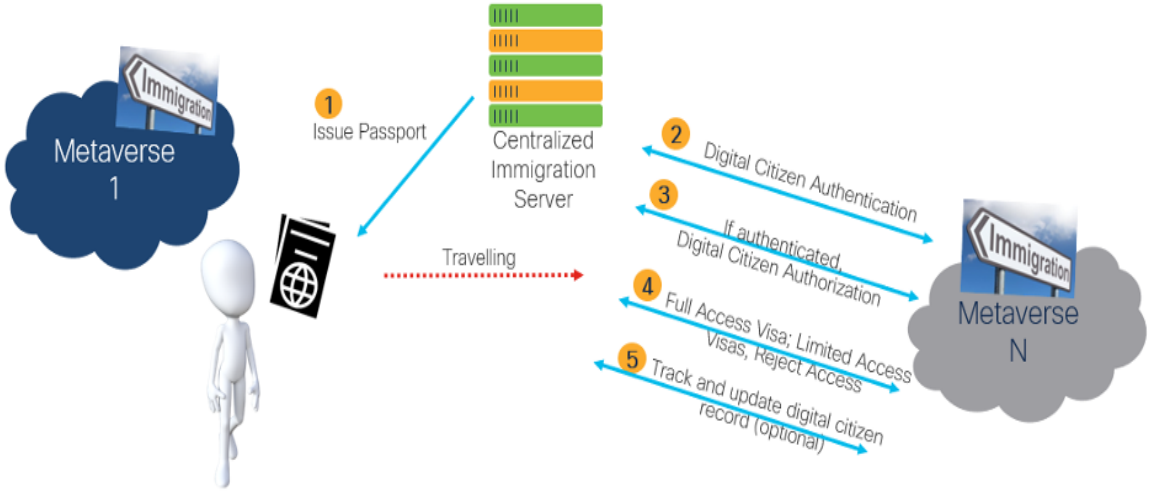

Figure 1: Passport Immigration Control for Travelling Between Metaverses

Figure 1, above, identifies a number of steps, which are labeled 1 through 5 in the figure, which are possible according to the techniques presented herein. Each of those steps will be described below.

A first step encompasses a digital citizen receiving a passport. When a digital citizen looks to travel to another metaverse and carry with them their avatar and associated metadata, a passport needs to be issued to the citizen by the current metaverse. That passport can then be used by other metaverses to authenticate the citizen and ensure compatibility and functionality.

The passport that is issued to a digital citizen may include an avatar username, an identifier of the metaverse that issued the passport, a date of issue, a date of expiry, the capabilities of the digital citizen (including, for example, the availability of extended reality (XR) tools for immersive experiences, a cryptographic wallet, non-fungible token (NFT)

objects, etc.), and a digital track record Uniform Resource Identifier (URI) for the digital citizen.

An exemplary digital citizen passport, which may be expressed in a JavaScript Object Notation (JSON) format, may encompass:

```
{
   "Digital-citizen-passport": "digital_citizen_passport_number",
   "Avatar Username": "username",
   "Issuing metaverse": "metaverse1"
   "Date of Issue": "YYYY-MM-DD”,
   "Date of Expiry": "YYYY-MM-DD",
   "version": "N ",
   "last-update": "YYYY-MM-DD HH:MM:SS:MSEC",
   "Capabilities ": " OS, CPU, RAM, Browser, AR, VR, bandwidth, crypto wallet, NFT wearables…",
   "Track Record URI”: "https://username.metaversedomain/digitalrecords",
   …
}
```

Each metaverse will host the passports of its citizens either locally (in closed system metaverses) or on a centrally accessible server (in open system metaverses).

A second step encompasses the checking of a passport as part of a digital citizen authentication process. Referring to the example that was introduced above, when a digital citizen travels from Metaverse 1 to Metaverse N, Metaverse N may first validate that it permits Metaverse 1 digital citizens and then validate the passport of the digital citizen either against a central repository (as shown in Figure 2, below, for travelling across open system metaverses) or with Metaverse 1 directly (as shown in Figure 3, below, for travelling across closed system metaverses).

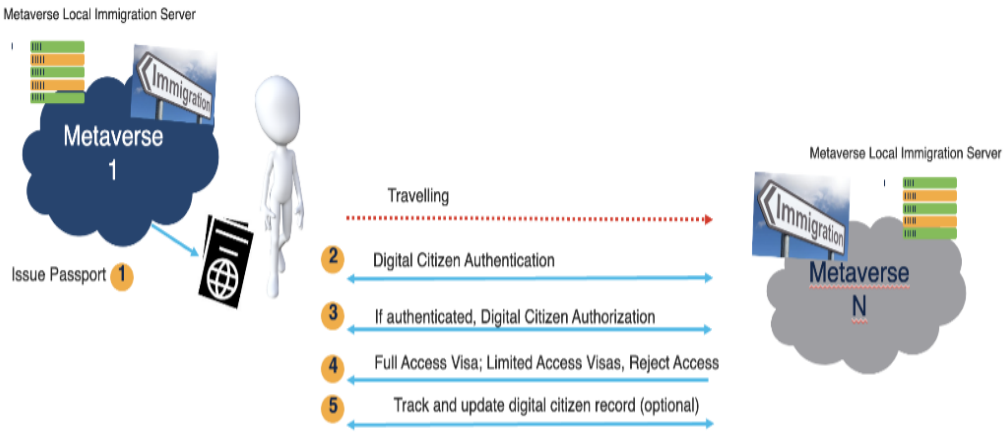

Figure 2: Digital Citizen Travelling Across Open System Metaverses

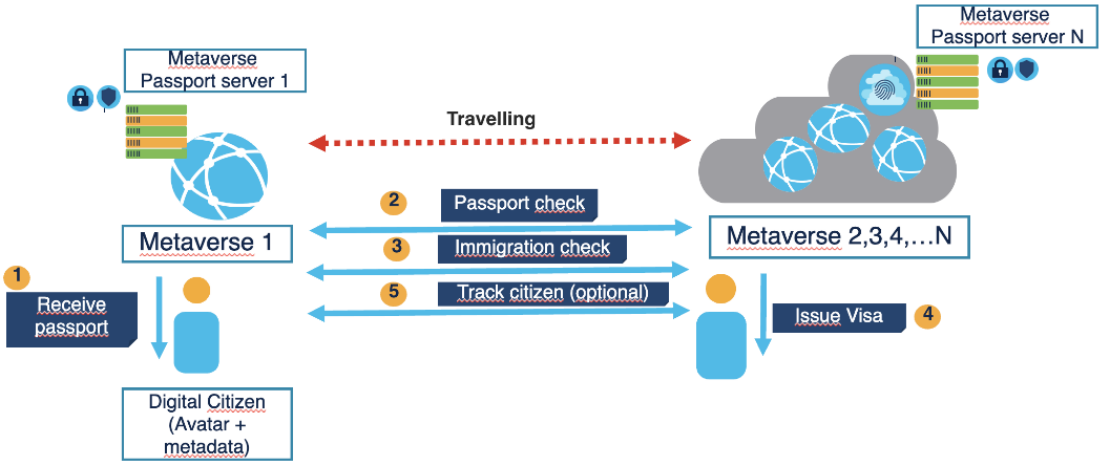

Figure 3: Digital Citizen Travelling Across Closed System Metaverses

The above-described process may be expressed in pseudo-code form as:

```
If (Metaverse 1 citizens are allowed in Metaverse N)
{
   A = Check Passport Number matches
   B = Check Passport is unexpired
   C = Check Passport Status is Unrevoked
   If (A AND B AND C = true)
      Result = call Immigration Check:
   Else
      Result = Fail
}
Else
```

```
Result = Fail
```

A third step encompasses an immigration check as part of a digital citizen authentication process. Each metaverse owner or administrator is responsible for defining the rules and regulations that a digital citizen must follow to gain entry to their metaverse.

Such rules and regulations may include endpoint requirements (such as operating system particulars, central processing unit (CPU) details, memory size, browser type, browser version, graphics card details, and augmented reality (AR) and virtual reality (VR) tools), network requirements (such as bandwidth, port numbers, etc.) and avatar requirements (such as a cryptographic wallet, NFT wearables, etc.) among others. A metaverse may define levels of these requirements which dictate the types of experiences that a digital citizen can gain access to within the metaverse.

Continuing with the example that was introduced above, following the authentication of a passport Metaverse N may examine the capabilities of the instant digital citizen. Those capabilities may be gathered during a passport check from Metaverse 1, or they may be gathered through an interaction with an avatar itself. The above-described process may be expressed in pseudo-code form as:

```
Immigration Check:
{
   ER1 = endpoint requirement1
   ER2 = endpoint requirement2
   …
   NR1 = Network requirement1
   NR2 = Network requirement2
   …
   AR1 = Avatar requirement 1
   AR2 = Avatar requirement 2
   …
}
```

A fourth step encompasses the issuance of a visa as part of a metaverse permitting or rejecting a digital citizen. Referring once again to the example that was introduced above, if all of the requirements are met then a digital citizen may be given a full access visa to Metaverse N. Otherwise, depending upon the specific requirements that are met, different

limited access visas may be issued to the digital citizen that will determine the type of experiences to which the digital citizen will have access. However, if the minimum requirements fail, then the digital citizen may be rejected, and they cannot join Metaverse N. An exemplary digital citizen visa, expressed in a JSON format, is shown below:

```
{
   "Digital-citizen-visa: "digital_citizen_visa"
   "Avatar_Username": "username",
   "Digital-citizen-Passport": "digital_citizen_passport_number",
   "Issuing metaverse": "metaverse2"
   "Date of Issue": "YYYY-MM-DD”,
   "Date of Expiry": "YYYY-MM-DD",
   "Visa-Type": "Full, Limited",
   "Limited-Visa-Type": "NoARVR, NoNDA,…."
   "Version": "N",
   "Last-update": "YYYY-MM-DD HH:MM:SS:MSEC",
   "Capabilities": "OS, CPU, RAM, Browser, AR, VR, bandwidth, crypto wallet,
NFT wearables…",
   "Enable tracking ": "yes, no”,
   "Track Record URI": "https://username.metaversedomain/digitalrecords",
…
}
```

A fifth step encompasses the tracking of a digital citizen as part of digital citizen accounting. A metaverse may choose to monitor the actions of a digital citizen during their time in the metaverse. Referring once again to the example that was introduced above, if Metaverse N wishes to account for the actions of a digital citizen, as part of issuing a visa it may trigger different tracking mechanisms including device profiling on endpoints (including AR or VR tools), user accounting, and generating or appending to the digital track record of the digital citizen. Such an updated track record may be shared by Metaverse N with Metaverse 1 or with any central service that is gathering a track record of digital citizens within the metaverses.

As described and illustrated in the above narrative, the techniques presented herein employ a passport and immigration system (shown in the above figures as a Metaverse Passport Server and a Centralized Immigration Server) to handle a digital citizen metadata capabilities negotiation process in support of seamless travel between metaverses. While

some existing approaches may work for more simplistic models where a user needs to log in to various places using a single identity, traveling between metaverses is more complicated and thus requires a more robust capabilities negotiation process.

Login credentials are the first step in allowing a digital citizen to travel across metaverses. Federated identity management (FIM) and identity and access management (IAM) approaches (which specifically talk of reusing login credentials across services and applications and role-based access control (RBAC)), or any other existing mechanism, can be used for credential verification. However, a digital citizen encompasses login credentials and metadata (such as an endpoint, network, and avatar capabilities as well as a digital citizen track record) that play into permitting access to a metaverse and the type of experiences within the metaverse.

The techniques presented herein support the type of capabilities exchange that was described above through a novel solution to the previously described challenge that will become more significant as metaverses evolve.

The presented techniques support a range of capabilities including, for example, endpoint capabilities; operating system details; browser type and version; AR and VR end device availability; the type of AR and VR devices in use; graphic card details; resolution; network capabilities; bandwidth measures; quality of service (QoS) requirements; port numbers; avatar capabilities; avatar creation services or method used; the presence of a cryptographic wallet (a compatible wallet could be a requirement); and NFT wearables, accessories, and skins.

For example, a metaverse that is targeted to children may tolerate all avatar types and have a minimal endpoint and bandwidth requirement. However, enterprise metaverses may require specific permissions (such as a non-disclosure agreement (NDA)) and AR or VR glasses for specific experiences. High-end gaming metaverses may well have stringent bandwidth and QoS requirements, along with minimal resolution support and graphics cards or VR glasses to deliver the experiences that are designed in their metaverse. The techniques presented herein allow for a digital citizen in one metaverse to cross over to another metaverse after confirming that certain minimum standards or requirements are met. Visas may then be issued with various levels of access permissions or restrictions.

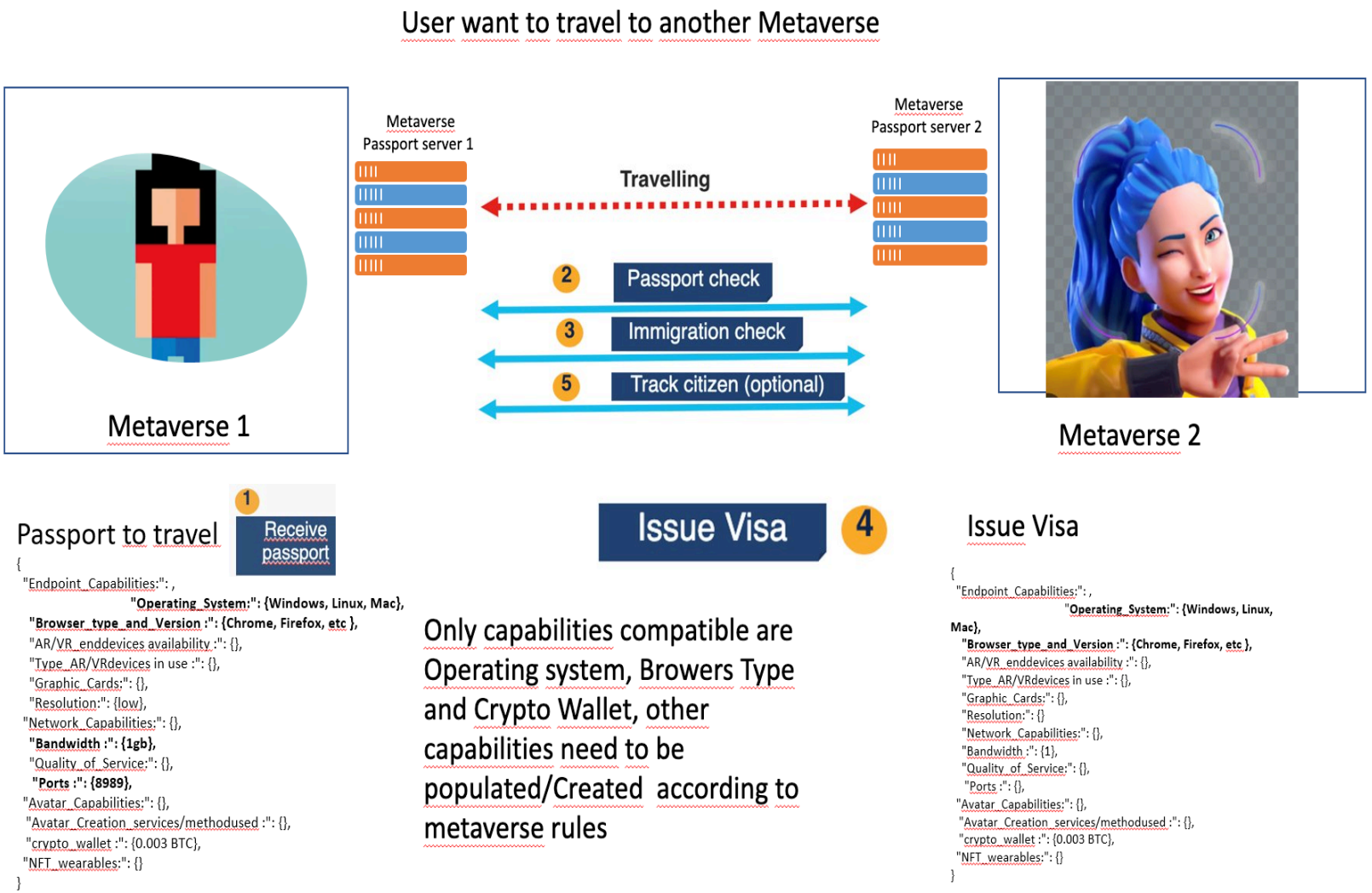

Figure 4: Example Capabilities Exchange Process

Figure 4, above, presents a more detailed depiction of a capabilities exchange process according to the techniques presented herein.

As noted previously, an important part of the techniques presented herein is the system that handles such capabilities exchanges and allows for an interoperability between various metaverses. Such an approach includes a centralized authority that can provide passport and immigration checks as a service for traveling across metaverses. Without the above-described techniques, a user would need to create new accounts or digital citizens in every metaverse that they wish to be a part of.

In summary, techniques have been presented herein that support a checkpoint for digital citizens that are traveling from one metaverse to another and that serve as a verification system on a centralized or distributed server. The presented passport immigration control framework allows digital citizens to travel to other metaverses outside their metaverse of origin, while protecting the rights of users as digital citizens. Such controls establish and strengthen mechanisms to monitor the impact of future liabilities, legislative enactments, and user accountability. The presented framework also provides guidelines for the best standards that entities may take while assessing identity and tracking for a digital citizen. Use of the presented techniques can safeguard protections for digital citizens in a metaverse and encourage an entity's customers to invest in business and benefit by adopting the presented framework.