Preprint from: **https://www.gipp.com/pub/**

C. Ihle, F. Deifuss, M. Schubotz, B. Gipp, "Towards Portable Identities in the Matrix Protocol" in Proceedings of the IEEE 42nd International Conference on Distributed Computing Systems Workshops (ICDCSW), 2022.

Towards Portable Identities in the Matrix Protocol

Cornelius Ihle
Department of Computer Science
University of Göttingen
Göttingen, Germany
ihle@gipplab.org

Fabian Deifuß
Data & Knowledge Engineering
University of Wuppertal
Wuppertal, Germany
deifussfabian@gmail.com

Moritz Schubotz
Mathematics
FIZ Karlsruhe
Berlin, Germany
moritz.schubotz@fiz-karlsruhe.de

Bela Gipp
Department of Computer Science
University of Göttingen
Göttingen, Germany
gipp@cs.uni-goettingen.de

***Abstract*—In this paper we present a cryptographic challenge-response authentication mechanism to enable portable identities within the Matrix protocol. Online instant communication systems like Matrix connect people in a convenient and cost-effective manner. However, most of today's communication infrastructure relies on inherently centralized infrastructure. Matrix currently, takes a federated approach instead. However, to fully decentralize the Matrix network, further actions must take place. Among others, a user's identity must be disconnected from the server they used to sign up and happen to communicate on. As part of this effort, a challenge-response authentication mechanism has been implemented that allows user IDs to be usable on any server, even if the a user's *homeserver* becomes unreachable.**

Keywords—instant messaging, challenge response mechanism, portable identities, authentication, self-sovereign identity

I. Introduction

Nowadays, most online, real-time communication protocols rely on centralized infrastructure. Besides the social aspect, decentralization offers greater resilience and horizontal scalability as opposed to centralized infrastructure. Matrix is a federated real-time communication protocol that anyone can extend by hosting their own server. However, each user's identity is tied to a specific server, their *homeserver*. This means that one's identity is controlled/owned by a specific homeserver, not by the individual. Assuming a server shuts down its services, all hosted identities become inaccessible. Currently, most users sign up at the "official" matrix.org homeserver as they expect the most stable experience. This implies a greater consolidation of homeservers, although further decentralization is desired. Thus, users should be able to communicate using the Matrix protocol even if their homeserver is unavailable[1].

To enable the migration of user identities, each identity has to be decoupled from its homeserver, allowing users to be self-sovereign. In the case of Matrix, each self-sovereign identity (SSI) shall be primarily used as a means of authentication, enabling the portability of identities across homeservers. As part of this effort, we implemented a challenge-response authentication mechanism [2] based on asymmetric cryptograghic key-pairs to enable portable identities within Matrix.

Background

A. Matrix

Matrix is an open-source project that publishes the Matrix open standard for secure, decentralized, real-time communication. Any communication adhering to the matrix protocol shares ownership of the conversation equally with all participants. Thus, each participant's server is self-sovereign. Matrix is more of a decentralized conversation store rather than a messaging protocol[2]. Sending a message inside a conversation ("Room") in Matrix replicates it to all servers that are part of said conversation. *Dendrite* is a second-generation open-source Matrix homeserver written in Go, which we base our experiments on.

B. Decentralization and Federation

Decentralization and federation are not opposing goals. Rather, federation can be leveraged to achieve a decentralized system. Decentralization can be described as the dispersion or distribution of function and powers[3] away from one central instance, federation merely describes the concept of interconnected networks. As for Matrix, federation describes the interconnectivity between multiple homeservers, often referred to as server to server communication. Specifically, homeservers exchange messages, events and profile information[4].

C. Self Sovereignty

There is no consensus of a scholarly definition for Self-Sovereign-Identifiers (SSI) and its underlying principles. Christopher Allen describes the vision of SSI as an enhancement of digital identities in that it enables trust while preserving individual privacy[5]. In SSI terms, digital identities shall be

[1] https://github.com/matrix-org/matrix-doc/ pull/2787
[2] https://matrix.org
[3] https://www.merriam-webster.com/dictionary/decentralization
[4] https://matrix.org/docs/spec/server_server/r0.1.4
[5] http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html

decentralized and "user-centric" as opposed to the "server-centric model of centralized authorities". Hence, individuals administer their own data individually, deliberately, and autonomously and take responsibility and control of their own identity and privacy. Leveraging decentralized identifiers ("DIDs") for SSI, the role of previously trusted and thus more privileged issuers, such as governments, are reimagined. [3]

II. Experiment

Most if not all Self-Sovereign-Identity designs evolve around asymmetric cryptographic methods of identification. Acknowledging this, a high level of interoperability can be achieved by sticking to low-level building blocks. The most critical security service that the challenge-response authentication mechanism achieves is Entity Authentication. Thus, an entity's ID can be established and verified safely. This is achieved by leveraging digital signatures.

To support digital signage within Dendrite Matrix server:

1. Each user needs to be identifiable by a single public key that must be known by all corresponding homeservers.
2. Each user must keep track of their private key as this can be used to represent their one true identity.
3. A challenge-response authentication mechanism must be designed and implemented.

A. Challenge Response User Authentication

A challenge-response authentication protocol consists of at least two parties of which one party presents a question ("challenge") and another party must provide a valid answer ("response") to be authenticated [4]. With Ed25519 [1] digital signatures, we created the authentication scheme in Figure 2. We assume that a user is already registered on a homeserver and then, (1) the user requests to authenticate/login, (2) the homeserver generates a unique challenge string that must be signed using the user's private key, (3) the homeserver responds with the generated challenge to the user that requested to login, (4) the user signs the challenge, (5) the user request to log in using the generated signature, (6) the homeserver verifies the signature's validity, and (7) the login attempt gets rejected or approved with the transmission of a generated access token.

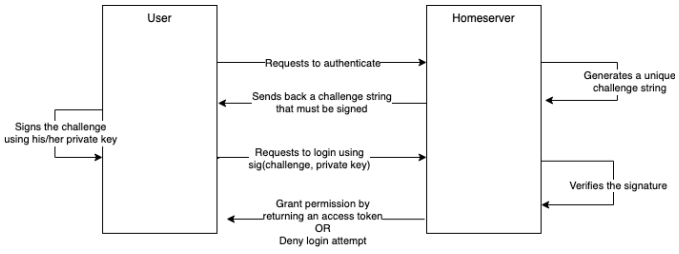

Fig. 1. Challenge Response Authentication

To accommodate the communication in an interactive authentication, each step of the authentication flow is split into specific stages. Each response made by the server then aids the user onto the next stage of the authentication flow until the authentication succeeds and an access token is returned.

We added the new Challenge Response User Authentication option to Dendrite's API to allow Matrix clients to utilize the server's new interactive authentication flow. In addition, we developed a small CLI-tool, so accounts can be created for testing purposes and without a full Matrix client.

To validate the implementation beyond unit tests, a live deployment has been rolled out that exposes the challenge-response authentication. Additionally, the deployment was validated locally. All code is available in the respective pull request to Dendrite[6].

III. Outlook

An authentication mechanism based on public-key cryptography does not enable fully portable accounts by itself. It is merely part of the more significant objective of having decentralized identities supported by the Matrix protocol. However, as long as future development uses public-key cryptography, the challenge-response authentication mechanism implemented in this paper can be used/referenced for client verification. Additionally, the login flow does not yet handle federation in case the user decides to switch their homeserver. Thus, self-sovereignty is yet to be achieved, but Matrix is one step closer to being fully decentralized.

IV. Conclusion

Our objective was to devise a challenge-response authentication mechanism within a Matrix homeserver reference called Dendrite[7]. Building upon the existing project, multiple classes have been extended and functionally modified to facilitate the authentication flow in question. To store an account's associated public key, the underlying database tables have been extended to accommodate the additional data. To aid the account creation process using the command line interface, we implemented a small helper utility. The API in question is not only reachable via the command line but also exposed over HTTP(S). For this, the login flow is now more extensible by making the login mechanisms configurable and differentiable at runtime. Finally, the functionality in discussion can be validated not only by the tests implemented but also by querying the live Dendrite deployment running in our laboratory.

References

[1] Bernstein, D.J. et al. 2012. High-speed high-security signatures. *Journal of Cryptographic Engineering*. 2, 2 (Sep. 2012), 77–89. DOI:https://doi.org/10.1007/s13389-012-0027-1.

[2] Beutelspacher, A. 2009. *Eine Einführung in die Wissenschaft vom Verschlüsseln, Verbergen und Verheimlichen.*

[3] Mahula, S. et al. 2021. With blockchain or not? Opportunities and challenges of self-sovereign identity implementation in public administration: Lessons from the Belgian case. *DG.O2021: The 22nd Annual International Conference on Digital Government Research* (Omaha NE USA, Jun. 2021), 495–504.

[4] Tilborg, H.C.A. van and Jajodia, S. eds. 2011. *Encyclopedia of cryptography and security*. Springer.

[6] https://github.com/matrix-org/dendrite/pull/2083

[7] https://github.com/matrix-org/dendrite