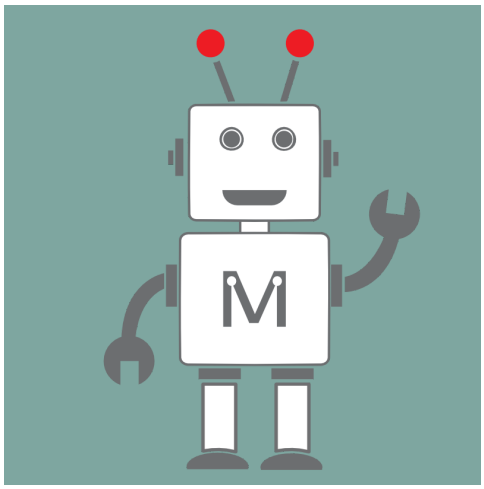
ENABLING GLOBAL DATA COMMUNICATION

SECURITY AND PRIVACY BY DESIGN



DECENTRALZED

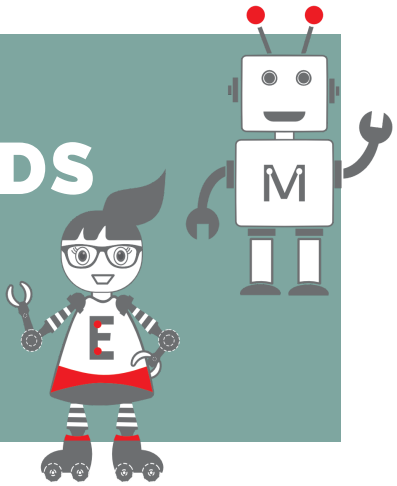
OPEN-SOURCE

Neuropil is the first open-source messaging protocol that is decentralized and comes with fully-automated security and privacy by design.
It enables highly secure, global data communication for communities dealing with sensitive information and which encourage data sovereignty and ZeroTrust security.

Neuro:pil

WWW.NEUROPIL.ORG

A PARADIGM SHIFT: TOWARDS ZEROTRUST SECURITY & DATA SOVEREIGNTY



CHALLENGE OF DATA PROTECTION

Data protection is tedious. It involves numerous stakeholders and blocks resources. In addition, frequently shifting data from on-premise to private/public cloud systems requires a continuous re-inspection of threat models. Multiple data ownership per device dismisses the assumption that we can design systems that are "safe and secure". Increasingly data sovereignty is on the agenda of the industry to protect intellectual property (trained AI algorithms), customer data (GDPR) and data provenance.

SECURITY AND PRIVACY BY DESIGN

As enterprise architects with a special interest in global data communication we have developed the first open-source messaging protocol that is decentralized and comes with fully-automated security and privacy by design. The best thing: We all have it in us! We named it after the fibrous network of tissue, which forms the gray matter in our brain. The biological neuropil facilitates networking between individual cells. In the same way Neuropil® assures the stable and secure communication between machines and applications. Neuropil® messaging layer reduces IT costs, maximizes availability, and increases reliability. The utilization of Neuropil® is diverse and can be implemented in all communities and organizations dealing with highly sensitive information, i.e. the healthcare industry,

TECHN. DETAILS

Neuropil® layer is a c-library, which is locally installed and embedded into your own application or devices. The lean messaging library is developed with two layers of encryption (transport and end-to-end). Neuropil gives each system involved a digital identity to avoid unauthorized access. All connected systems can be addressed distinctly through their digital identity. Data exchange is individually defined and controlled via attributes. Due to these cryptographically secured attributes data misuse is nearly impossible. A main benefit of Neuropil's decentralized approach is reliability. In case one actor in the system goes down, another party is addressed to „jump in“ and communication continues smoothly. In the decentralized network any party can be reached, even if there is no direct connection. Traditional messaging systems cover the horizontal value chain within a single enterprise and its internal connections. Neuropil can work throughout different organizations and systems, greatly reducing legislative burdens. At the same time, communication channels can be governed centrally. This offers great potential in the multi-tenant environments we are working in and opens the door for new collaborative business models.

https://neuropil.org
https://gitlab.com/pi-lar/neuropil
neuoropil@pi-lar.net
Developed @pi-lar GmbH

Neuro:pil