Neuro:pil

secure messaging

facts & fiction

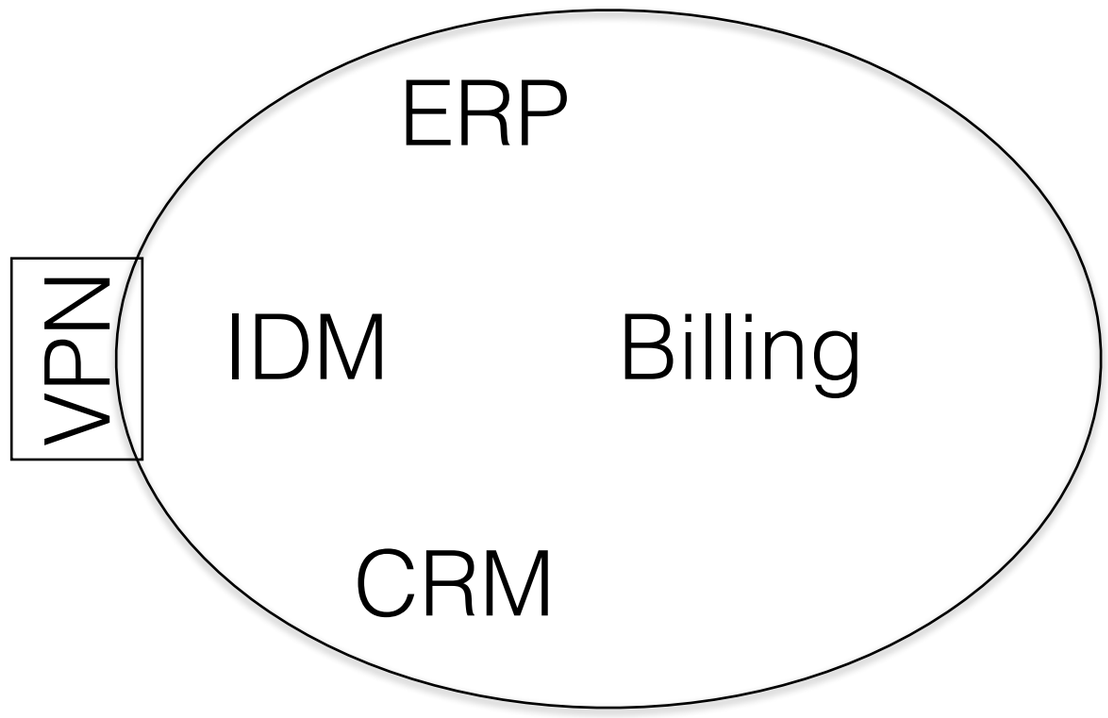
Mail
Web

MDM

PayPal

Neuro:pil
secure messaging

?

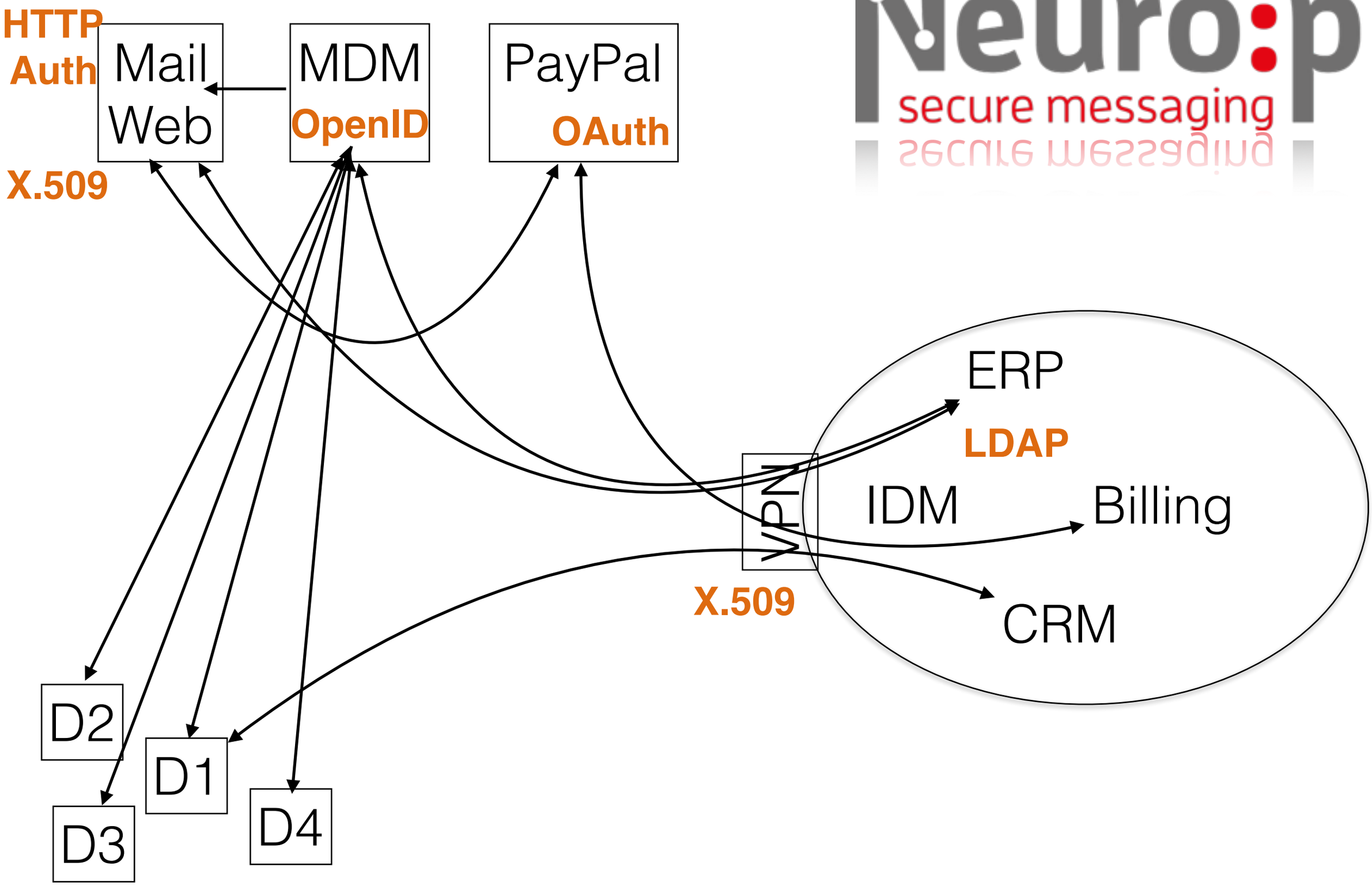


D2
D1
D3
D4

Industrie 4.0 ?

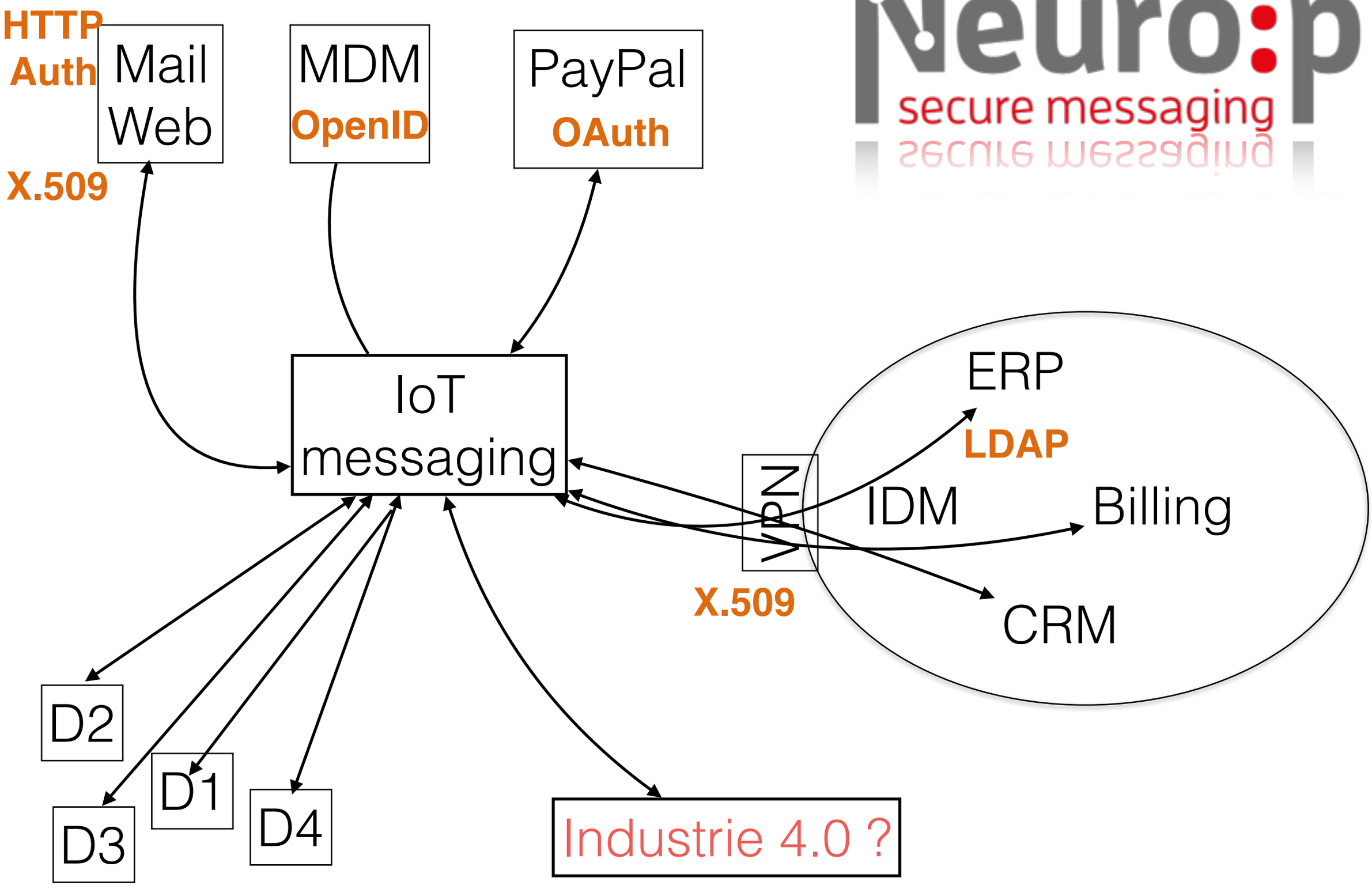
how do you connect n different system with each other ?

heterogenous networks / subnets / authentication / authorization / legal entities



connect everything with everything ?

technology stacks promote themselves / no governance



Neuro:pil
secure messaging

facilitate a central platform which acts as a central hub?

at least the technology stack problem is partly solved :-/

Neuro:pil
secure messaging

other vendor / open source projects to enable a central hub:

- mqtt / ZeroMQ / RabbitMQ / ActiveMQ / JMS
- IronMQ / Ice-T / EMS

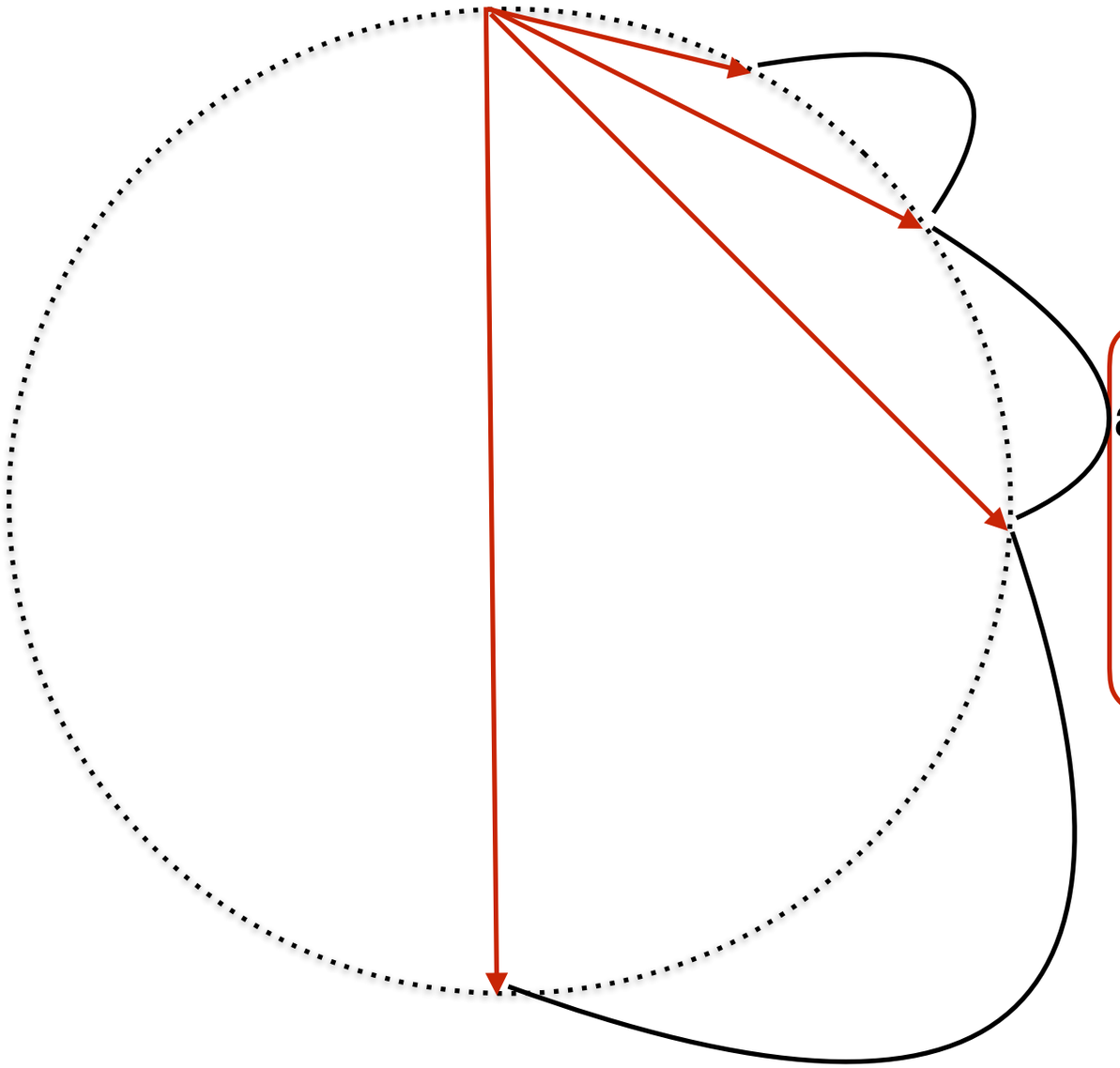
- but none of those really solves the problems outlined above

neuro:pil is an IoT / M2M messaging library

but with the main focus on:

- security first (end-to-end encryption)
- no single point of failure / attack
- decentral messaging / central governance

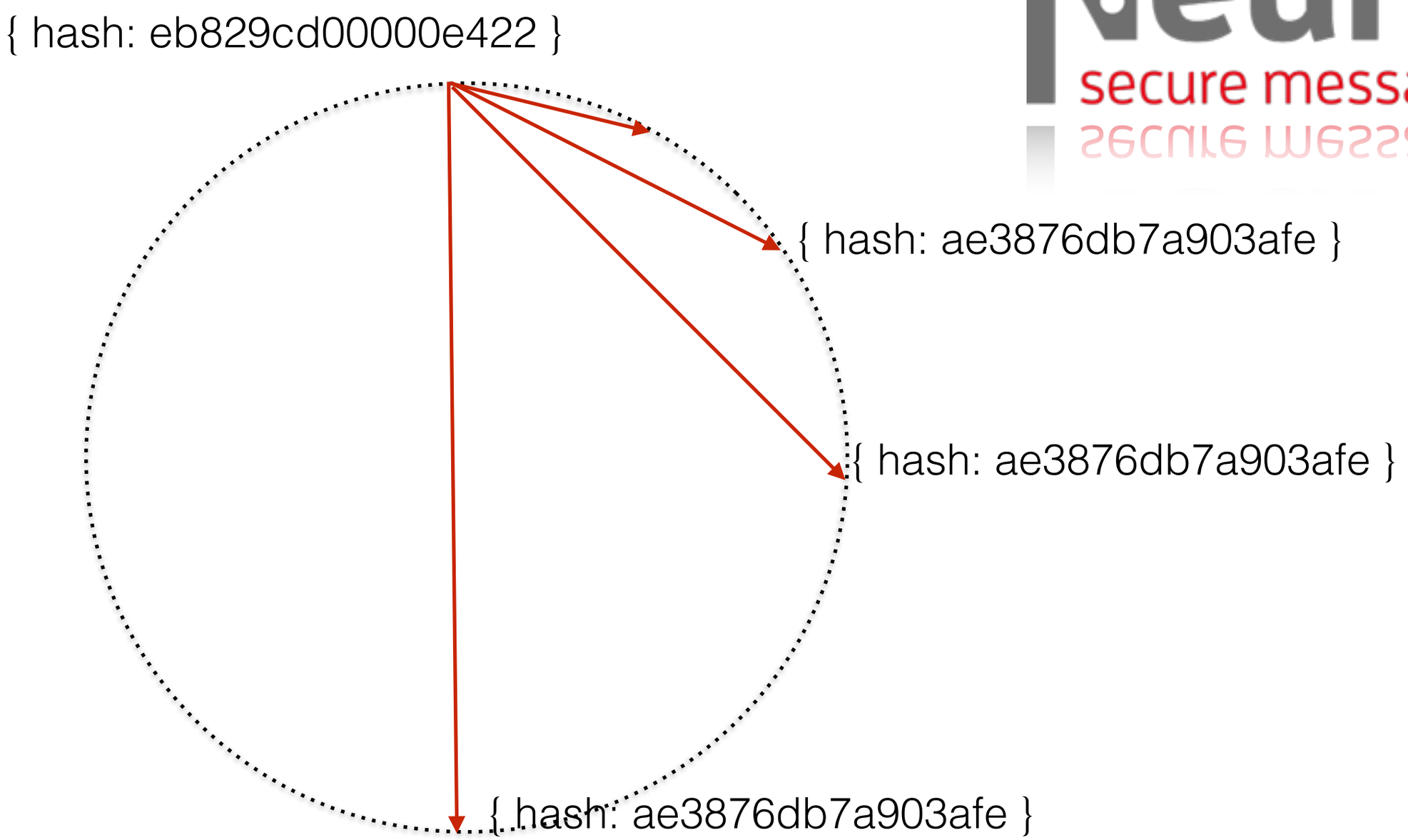
Neuro:pil
secure messaging



authenticated Diffie-Helman key exchange
pub_key: <binary data>
signature: <binary data>

in **neuro:pil** each participant connects to n neighbors
all nodes form a DHT serving as a secure overlay network
no single point of failure / dynamic addition / removal of new nodes

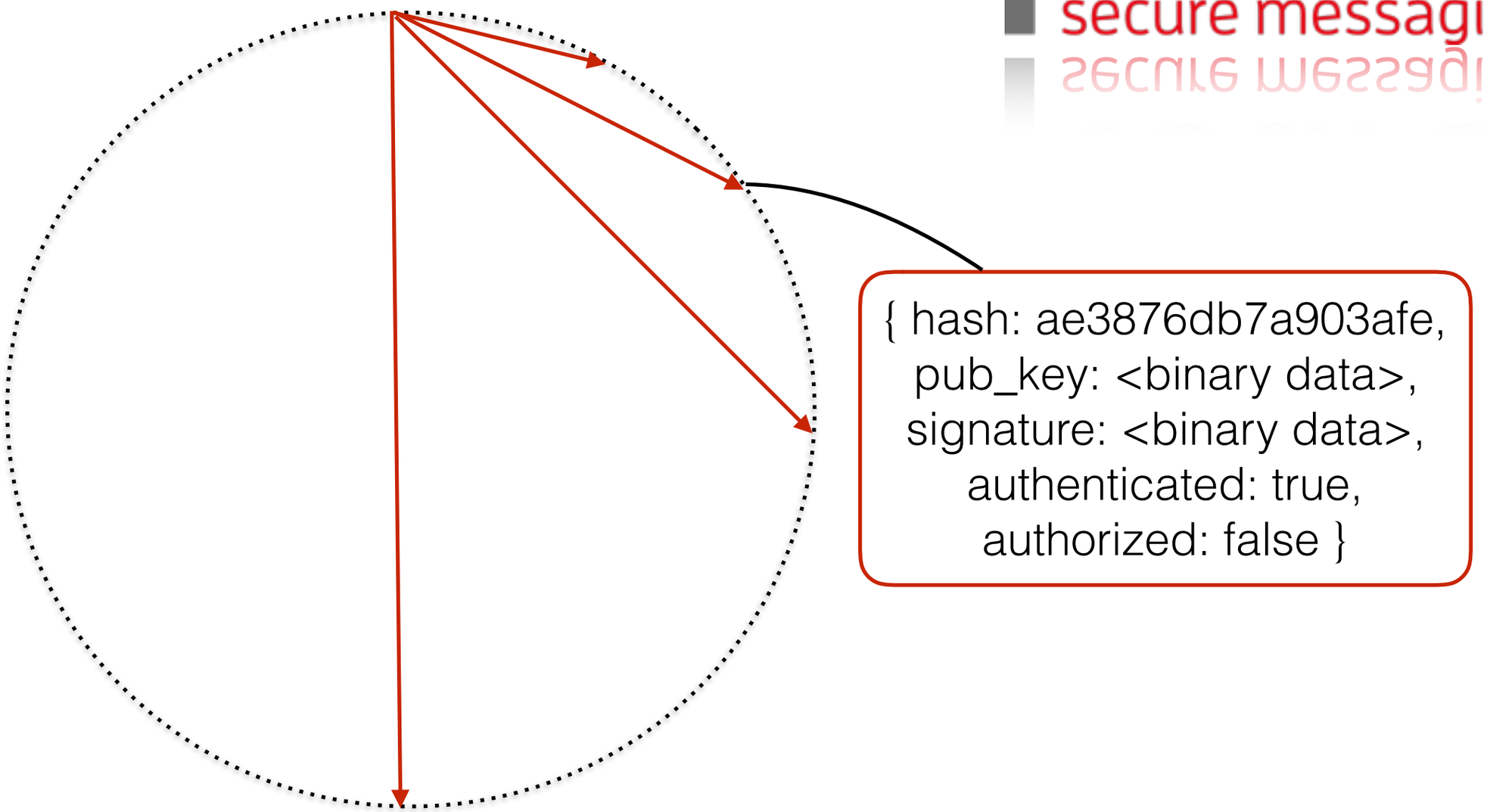
Neuro:pil
secure messaging



in **neuro:pil** addressing is based on hashes

- message subjects / data storage
- identity forwarders / authenticators / authorization
- no additional name lookup

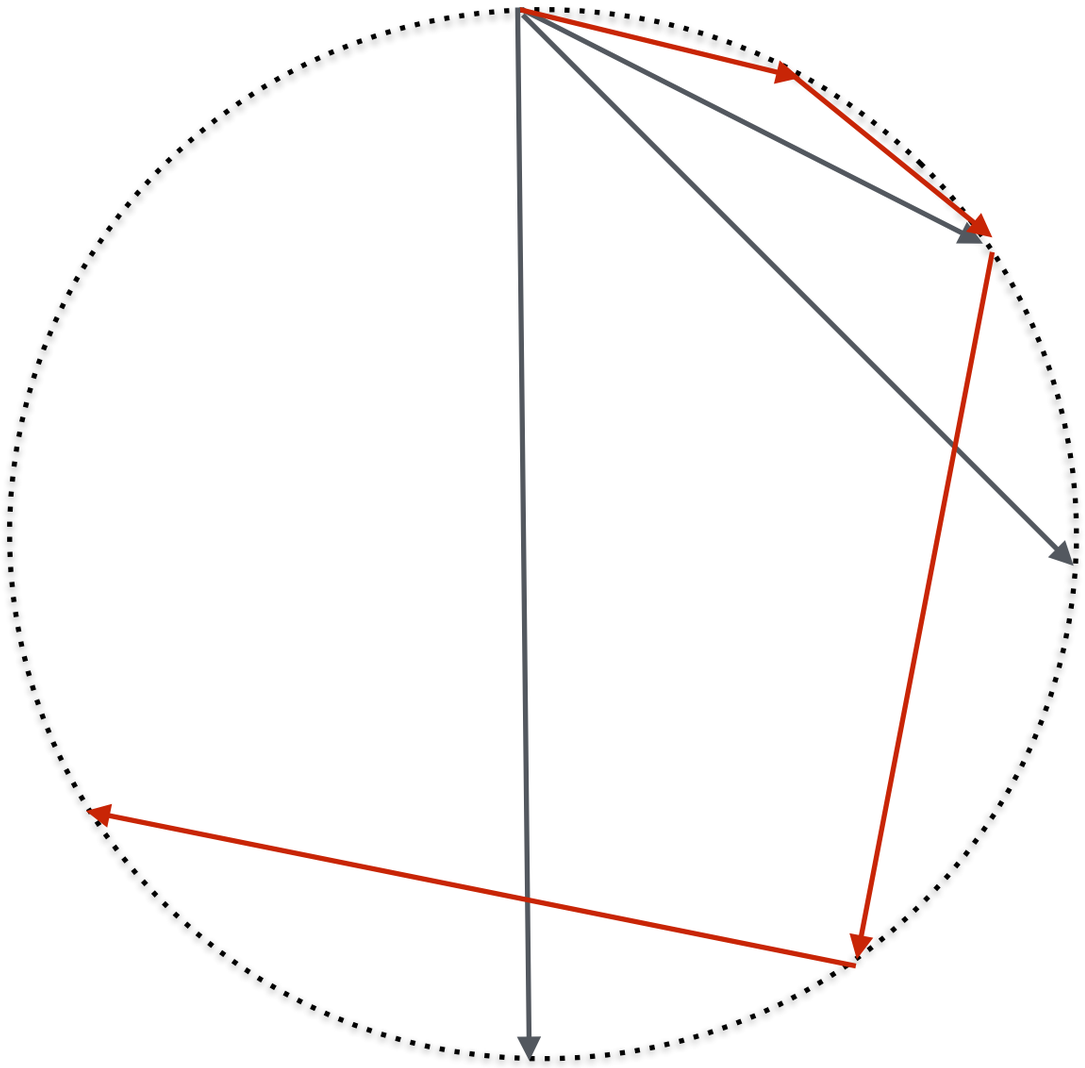
Neuro:pil
secure messaging



in **neuro:pil** participant exchange security tokens

only when nodes can authenticate / authorize tokens further communications or actions are established

Neuro:pil
secure messaging



in **neuro:pil** messages travel along to the target node

messages are chunked and forwarded to the next closest hash key
until finally reaching the destination.