The Future of Microservices Security

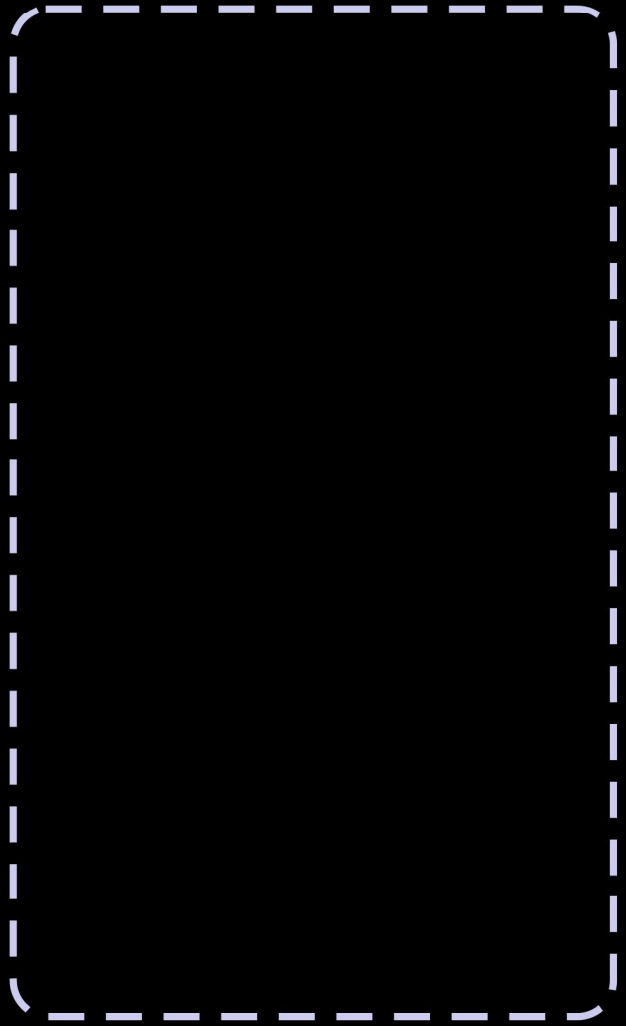
Eric Karge
Martin Kirst

Entwickler @Hypoport #Berlin

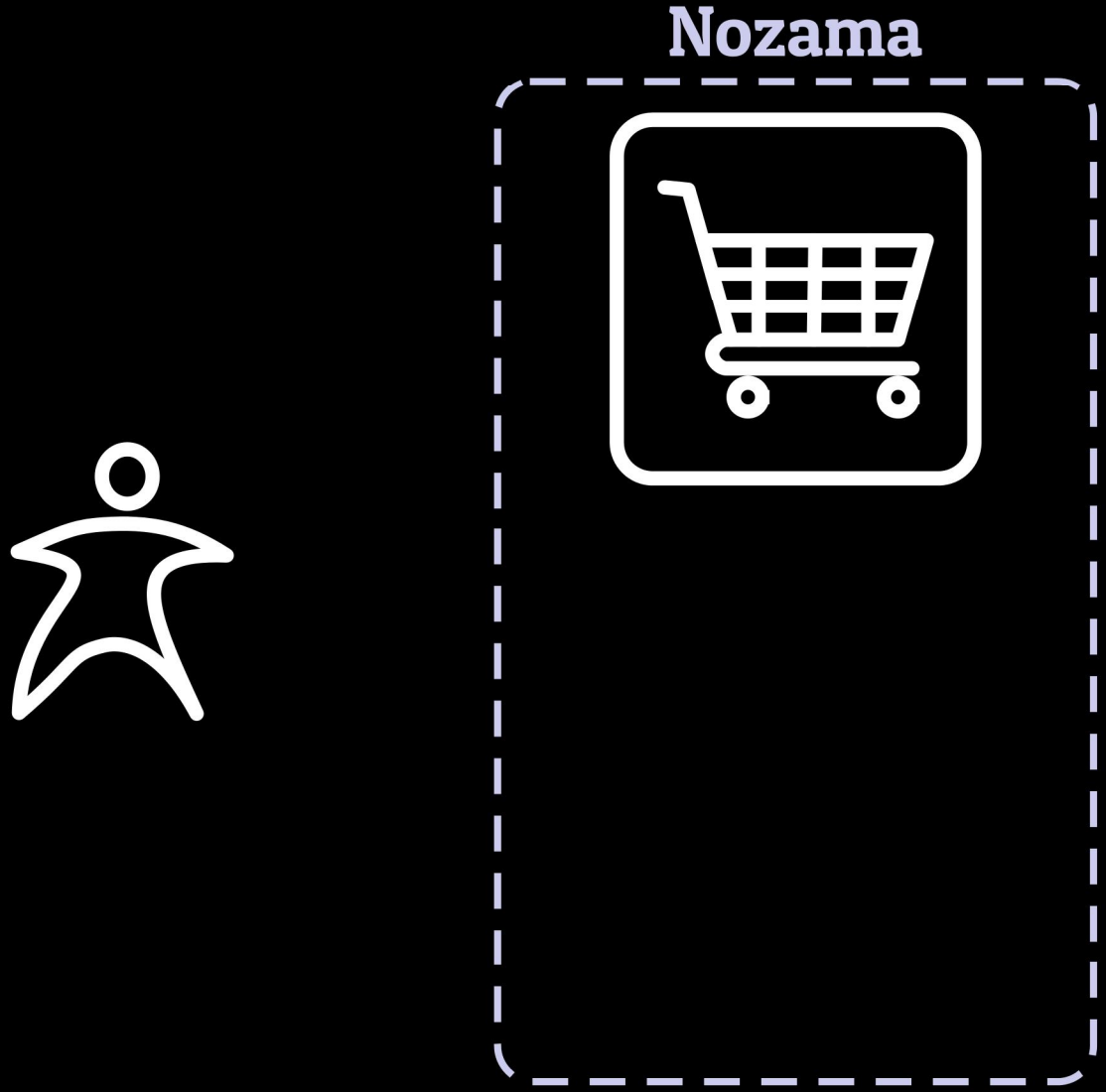
Motivation

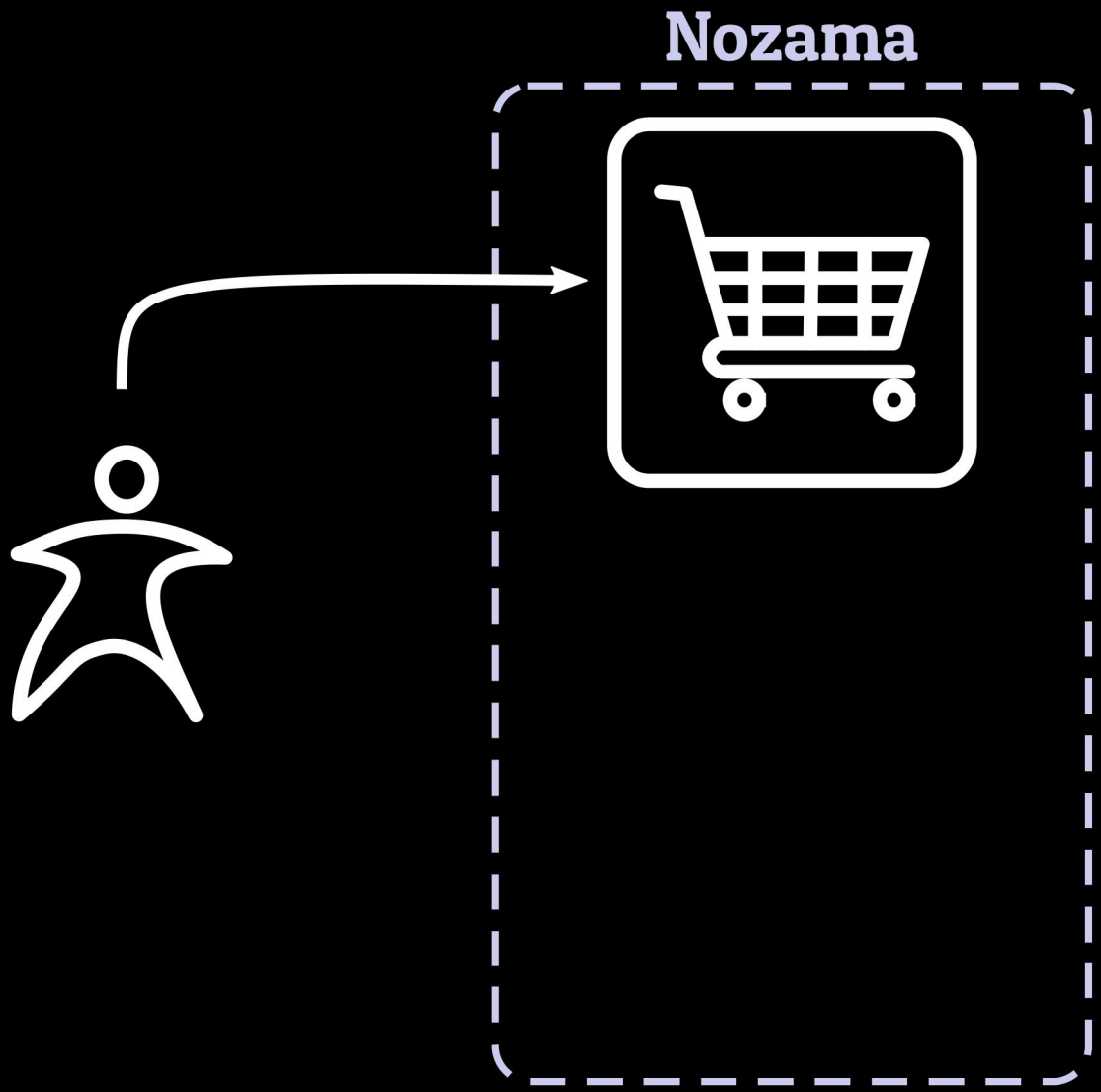
Demoszenario

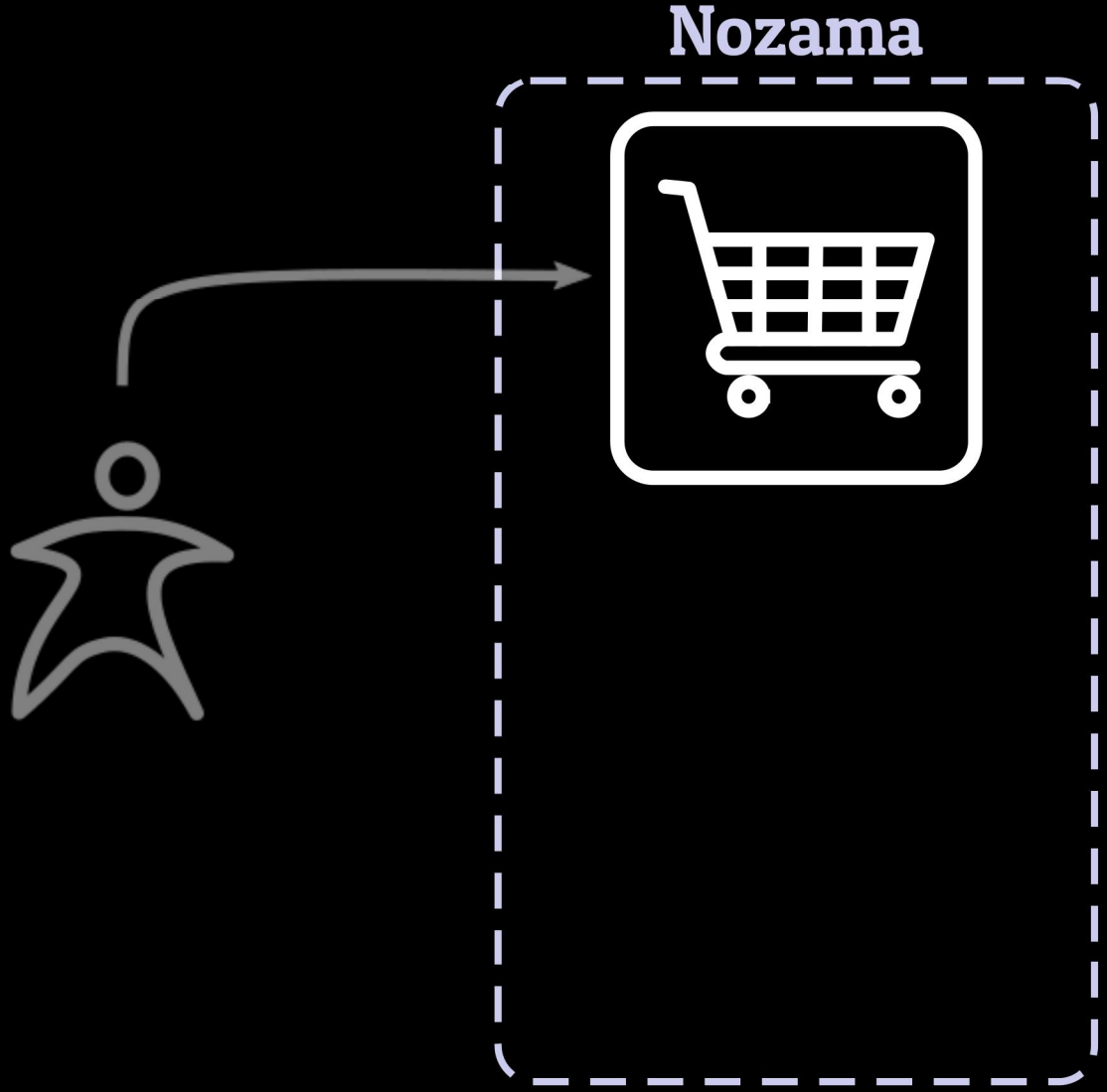
Nozama

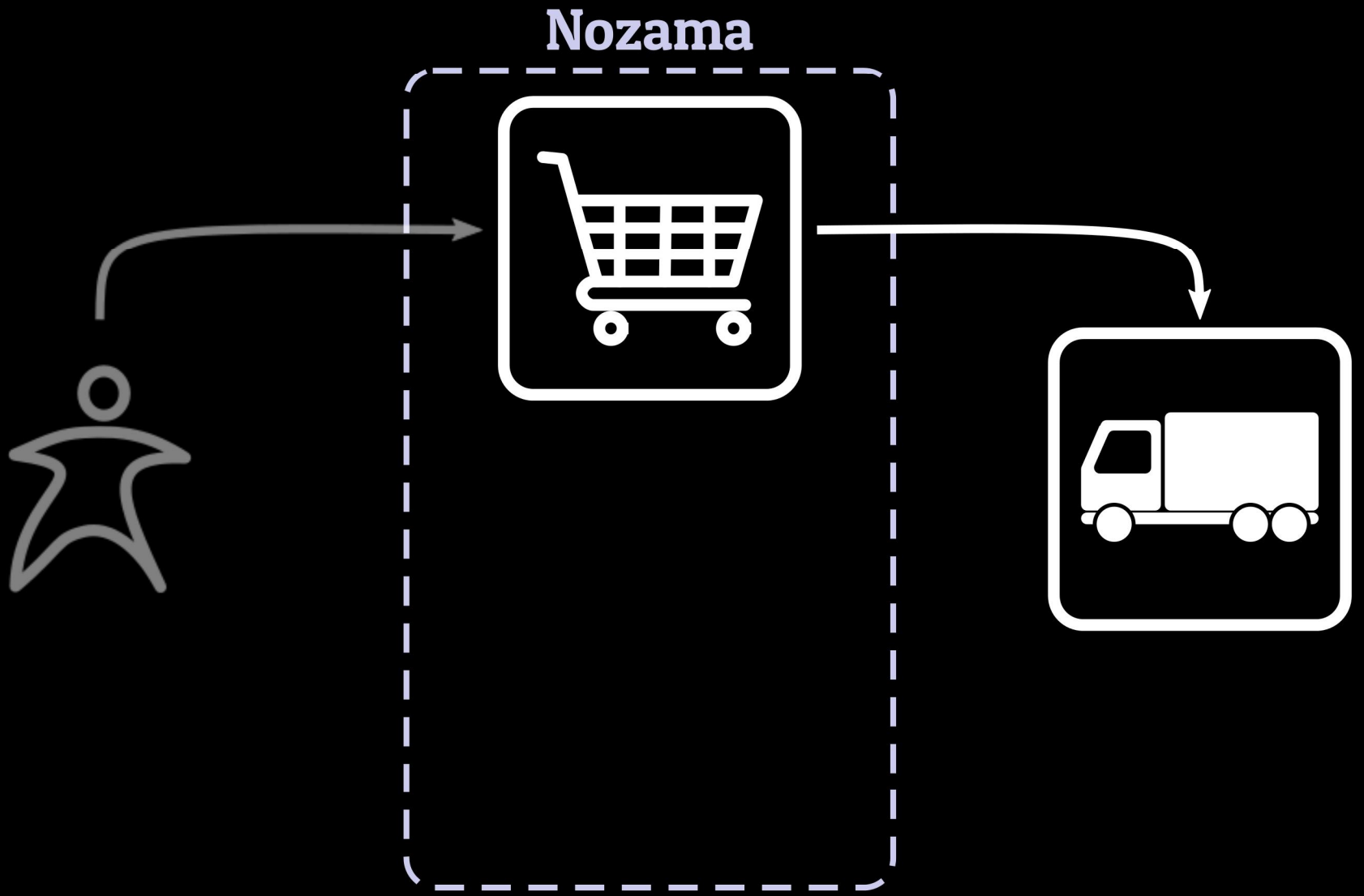


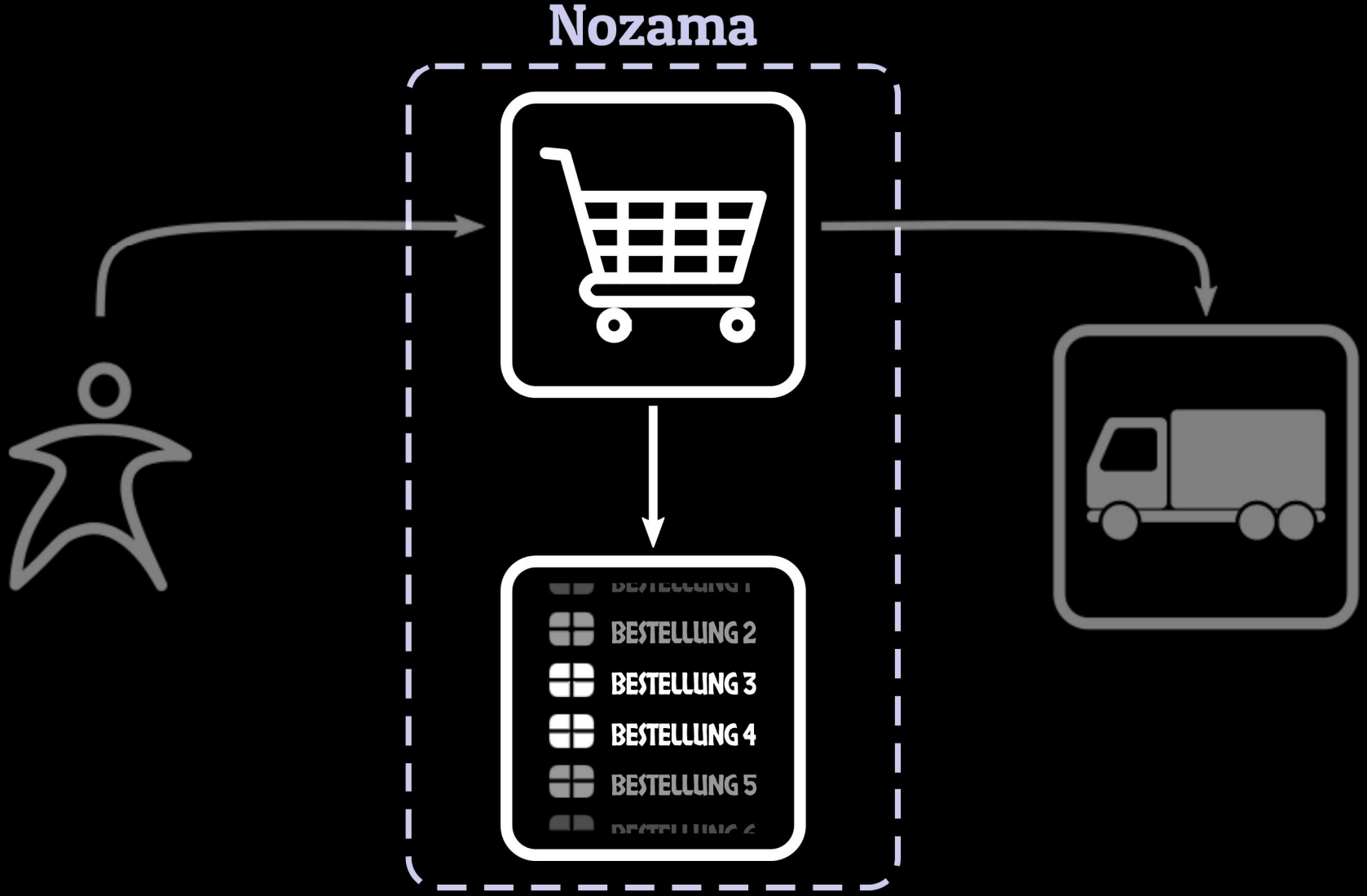
Nozama

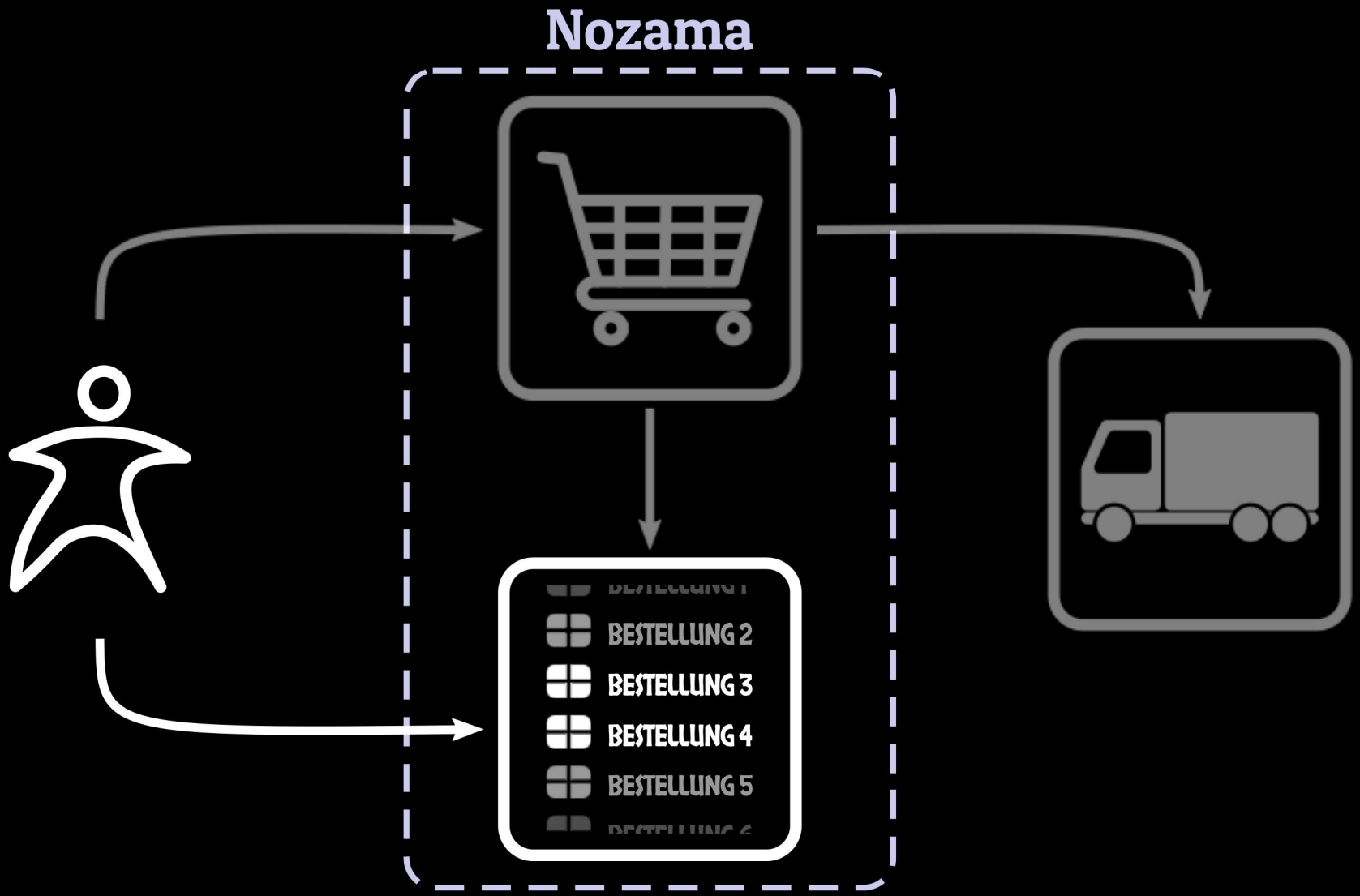

Nozama

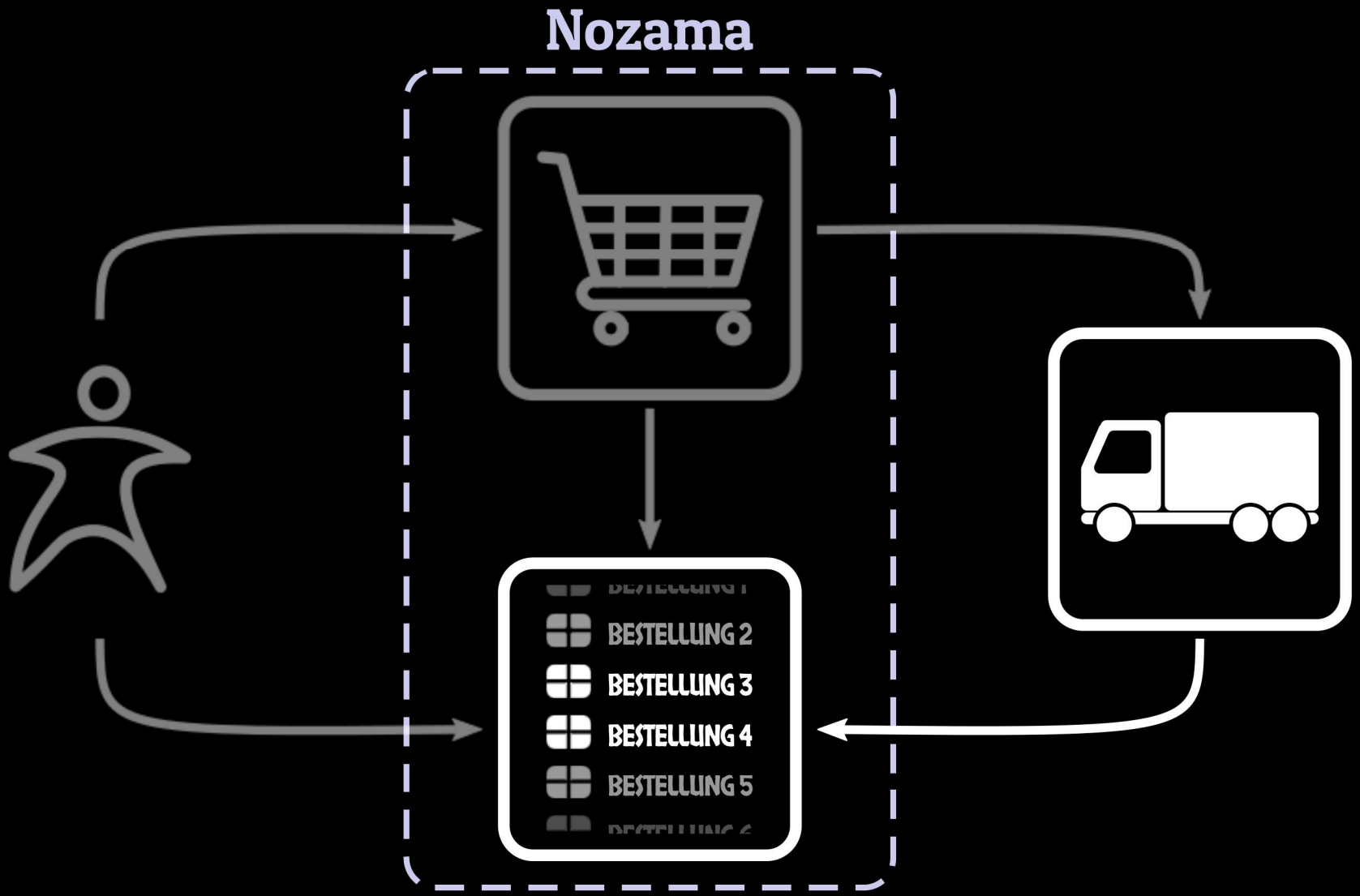

Nozama

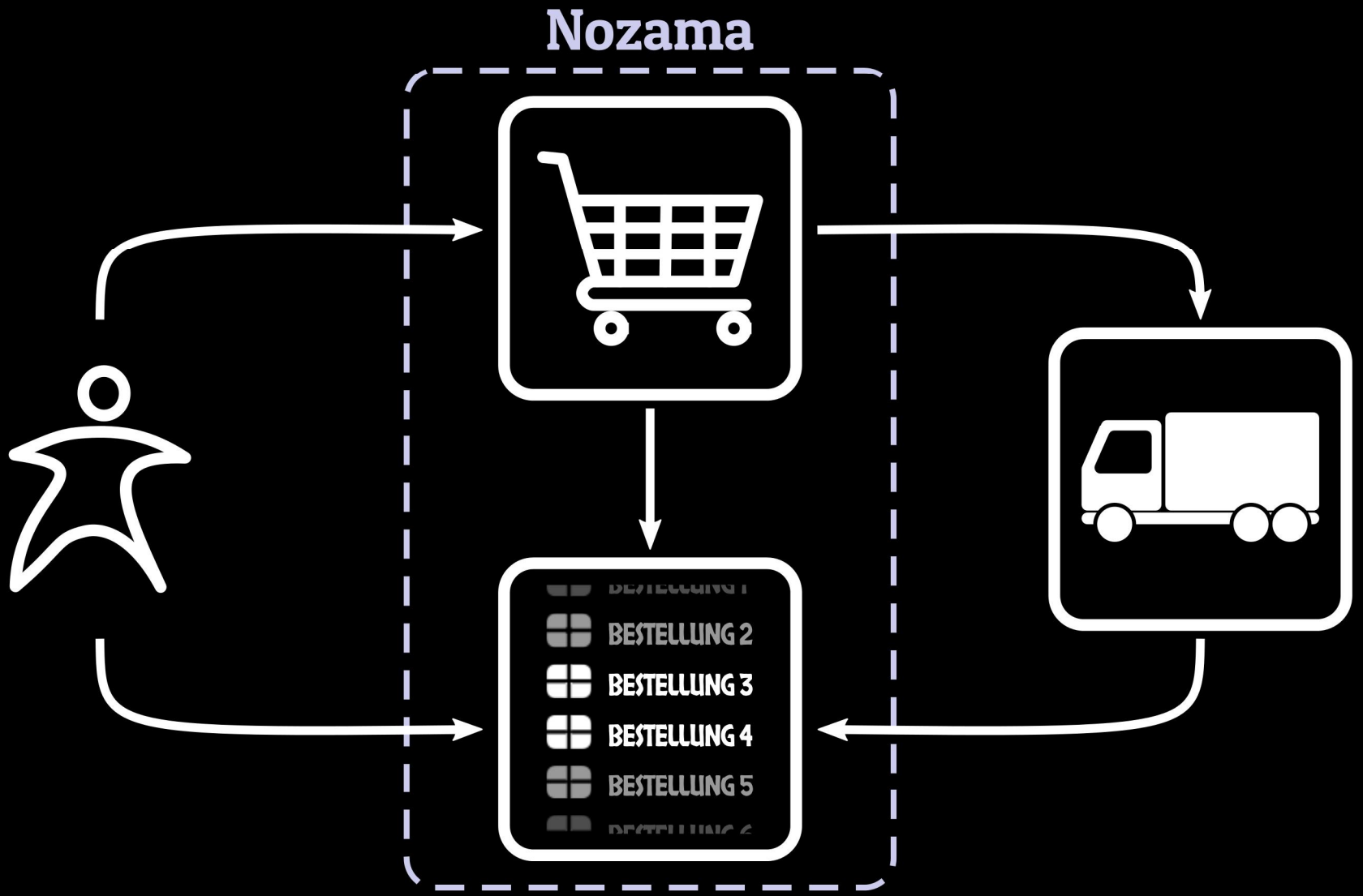

Nozama


Nozama


Nozama
BESTELLUNG 2
BESTELLUNG 3
BESTELLUNG 4
BESTELLUNG 5

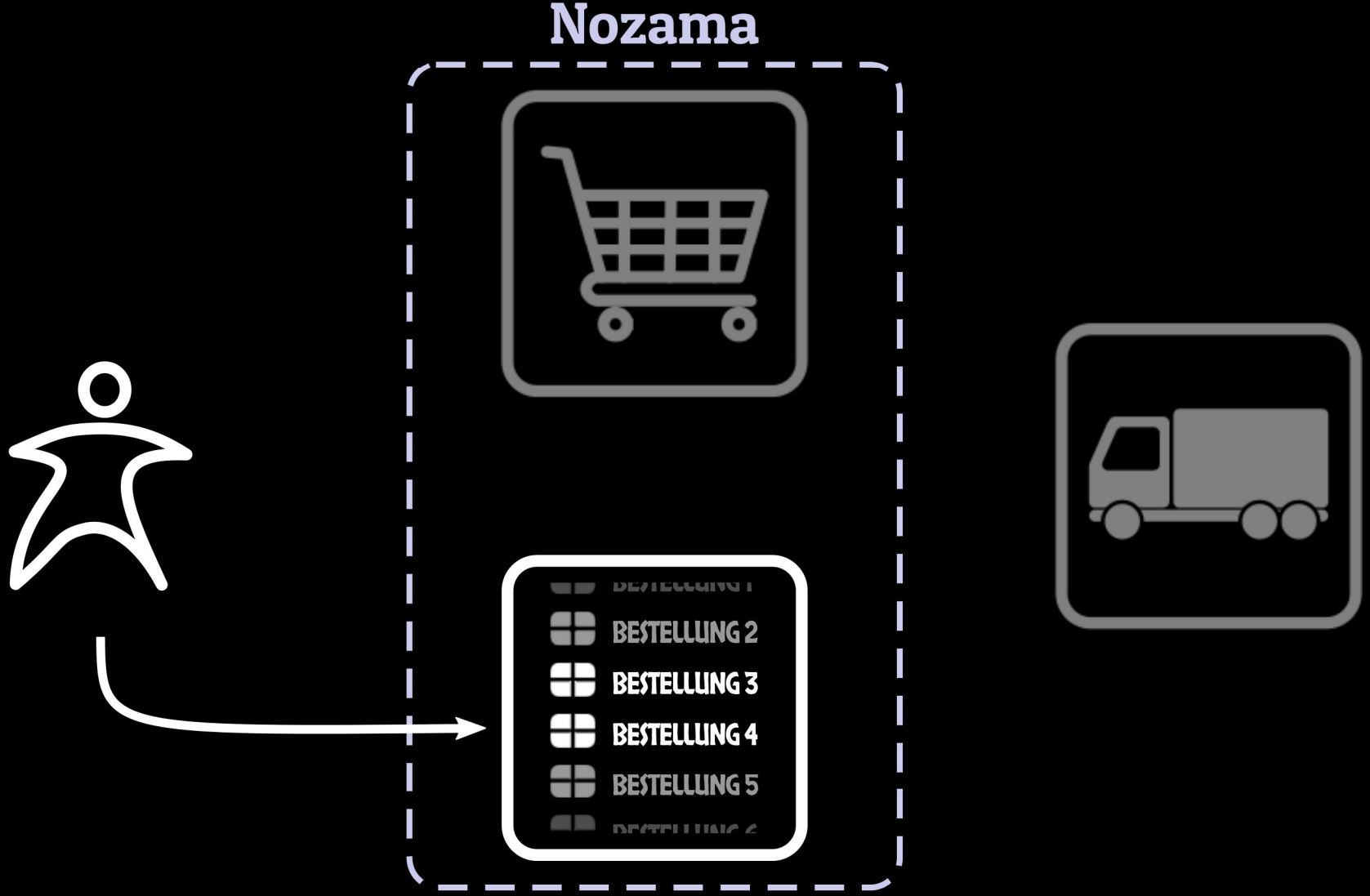

Nozama
BESTELLUNG 2
BESTELLUNG 3
BESTELLUNG 4
BESTELLUNG 5

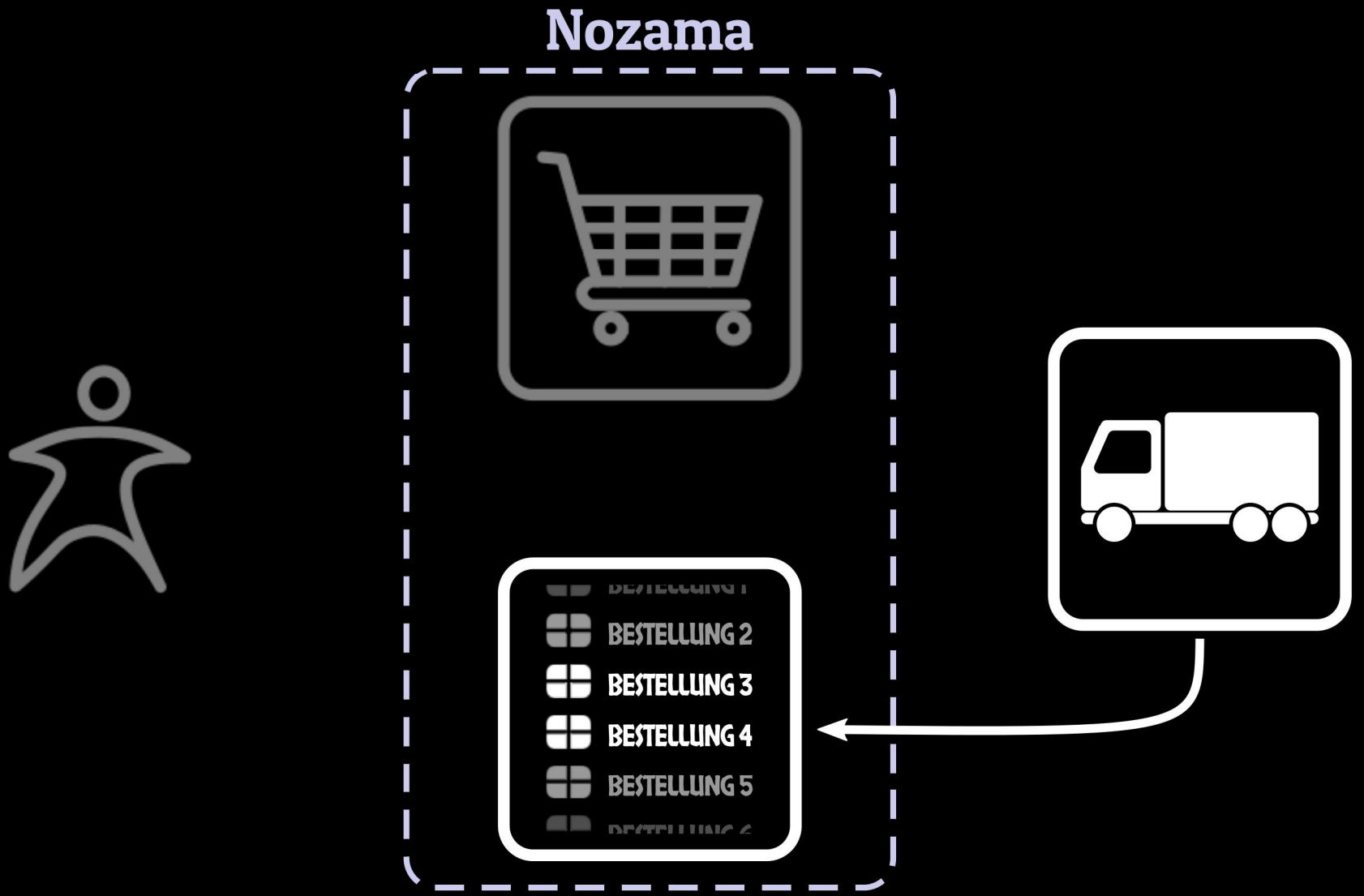

Nozama
BESTELLUNG 2
BESTELLUNG 3
BESTELLUNG 4
BESTELLUNG 5

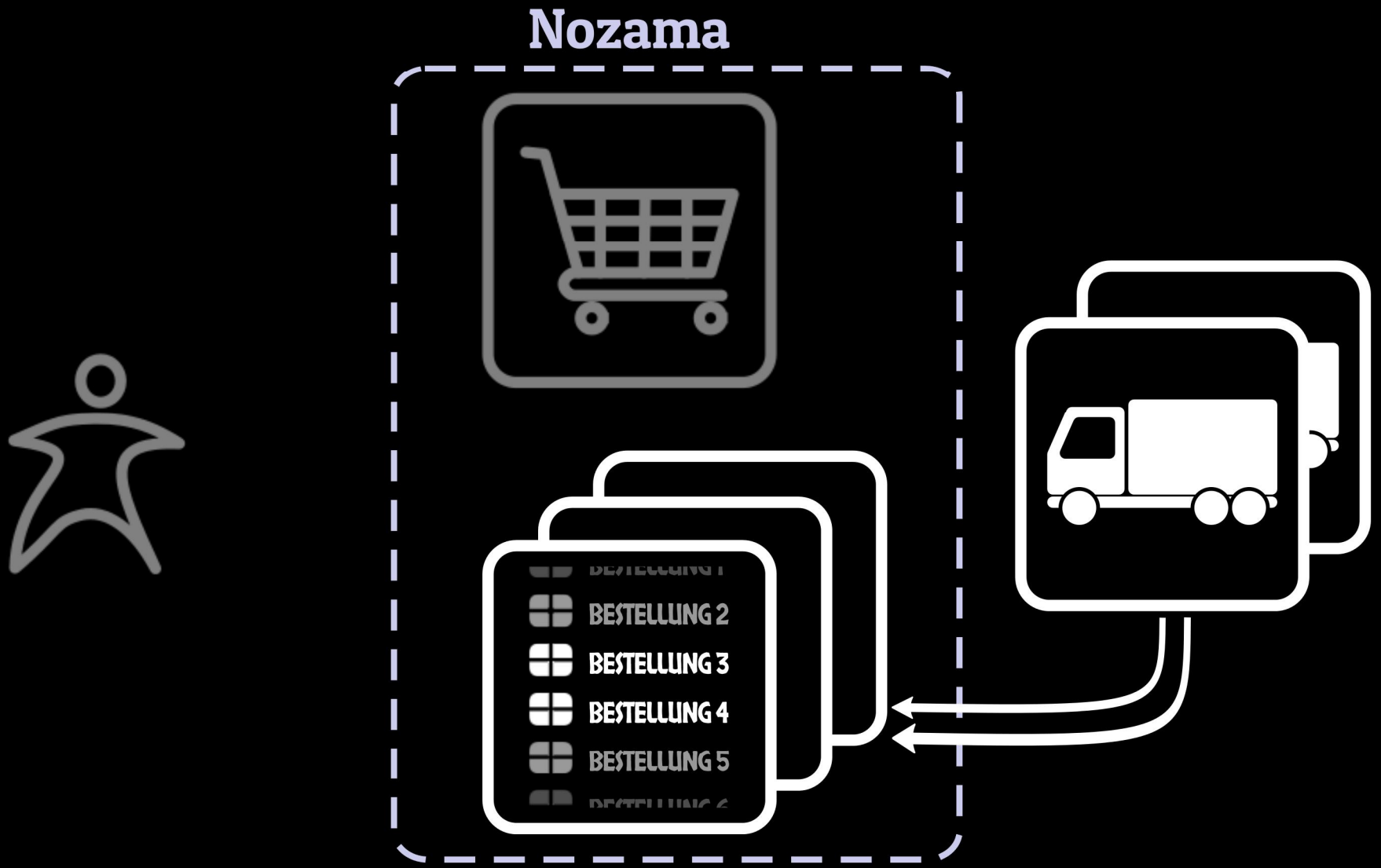

Nozama
BESTELLUNG 2
BESTELLUNG 3
BESTELLUNG 4
BESTELLUNG 5

Architektur


Nozama
BESTELLUNG 2
BESTELLUNG 3
BESTELLUNG 4
BESTELLUNG 5


Nozama
BESTELLUNG 2
BESTELLUNG 3
BESTELLUNG 4
BESTELLUNG 5


Nozama
BESTELLUNG 2
BESTELLUNG 3
BESTELLUNG 4
BESTELLUNG 5


Nozama
BESTELLUNG 2
BESTELLUNG 3
BESTELLUNG 4
BESTELLUNG 5

Zugriffskontrolle!

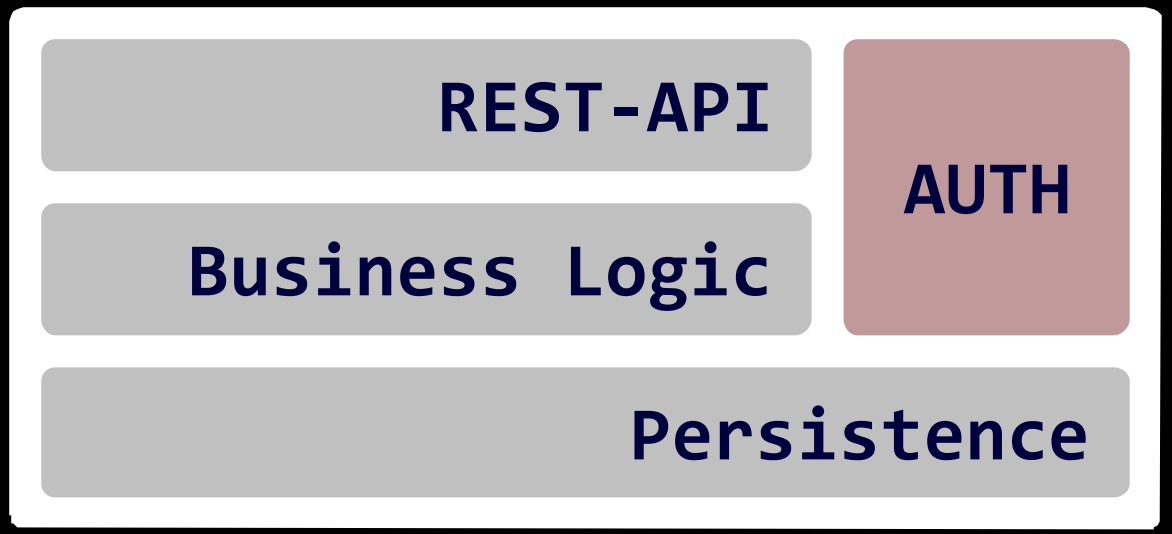
Zugriffskontrolle folgt Conway's Law

"Any organization that designs a system (defined broadly) will inevitably produce a design whose structure is a copy of the organization's communication structure."

Melvin E. Conway

Zugriffskontrolle im Softwarestack

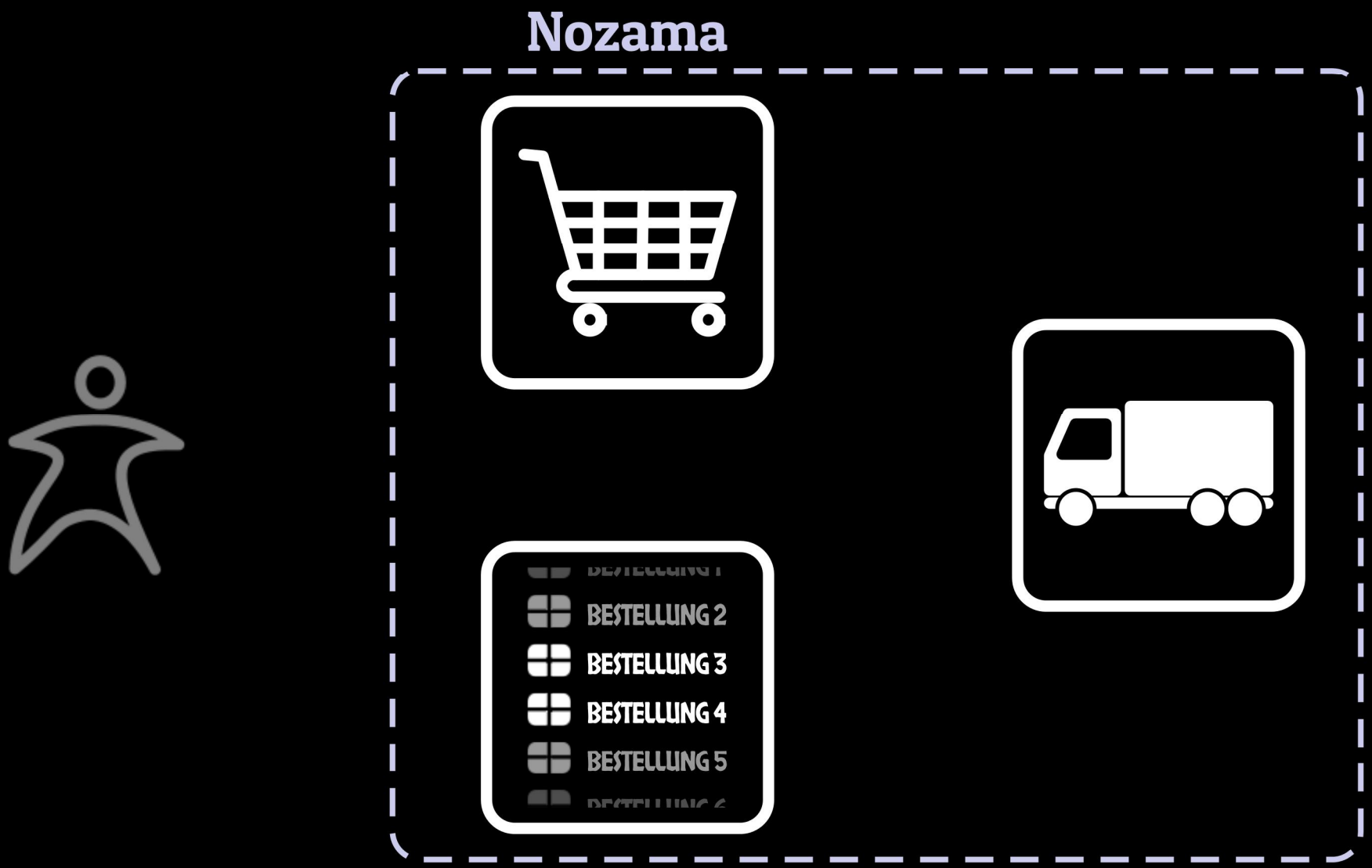
Zugriffskontrolle im Softwarestack



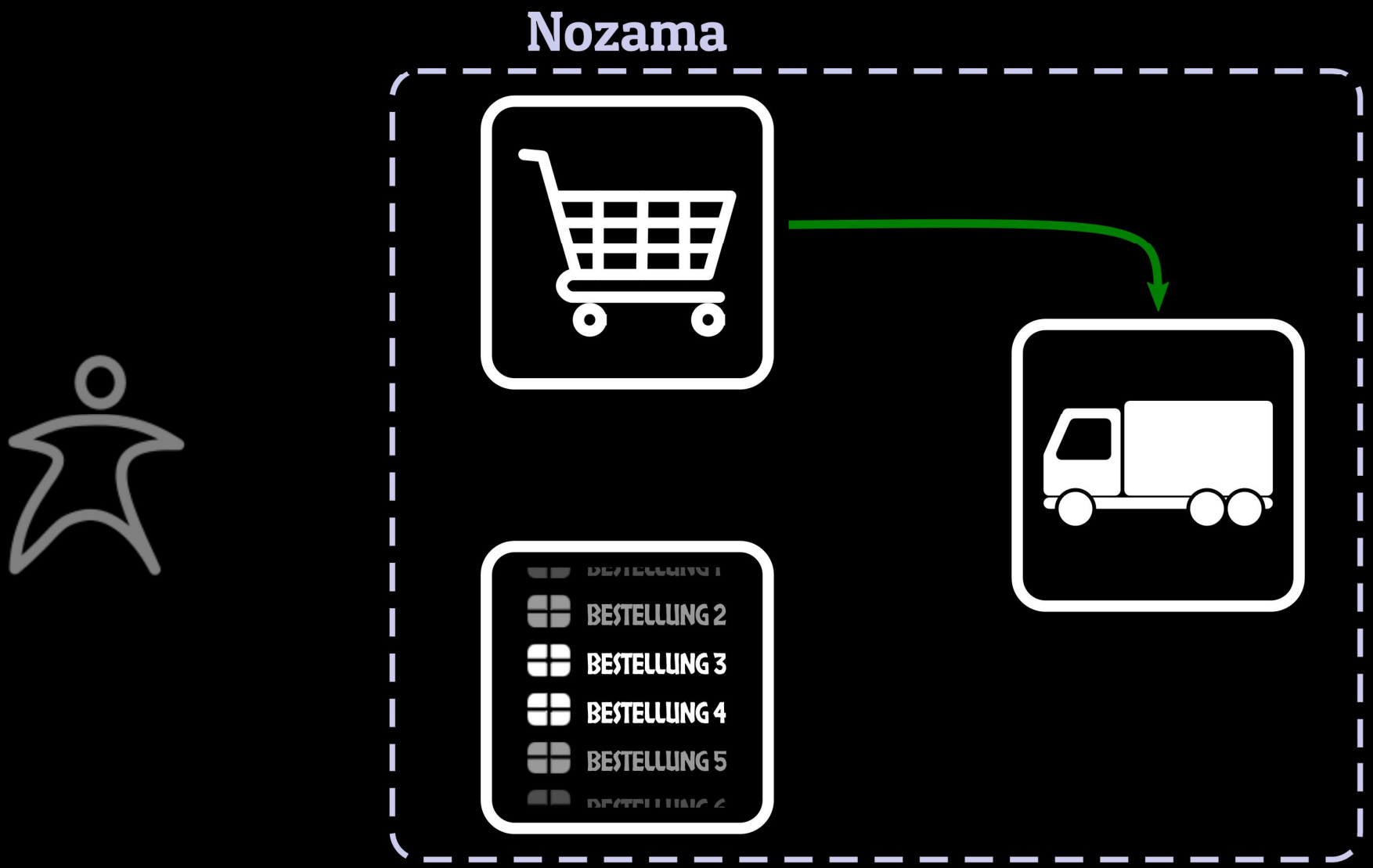
Zugriffsmodelle

Zonenbasiert

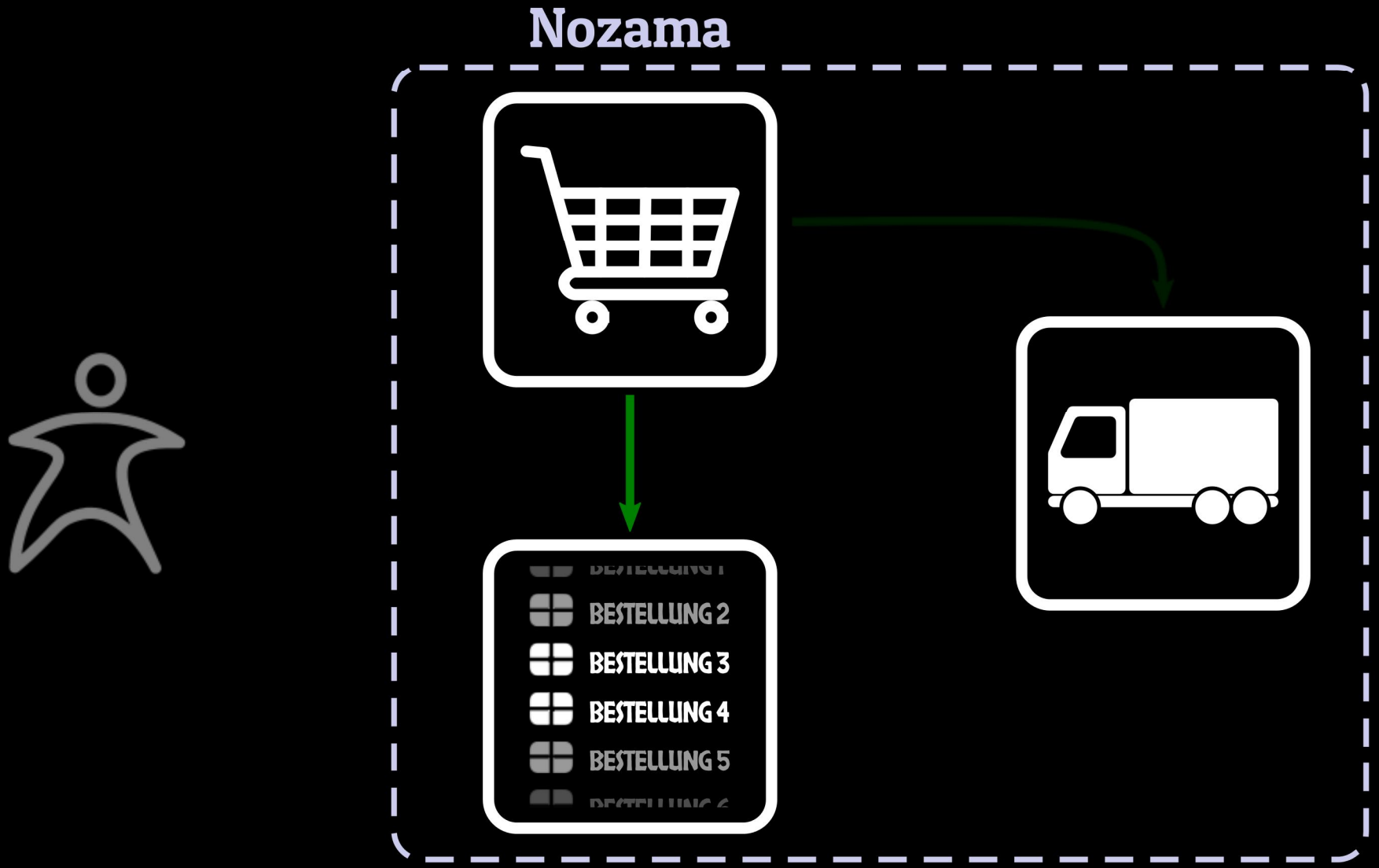
Zonenbasiert



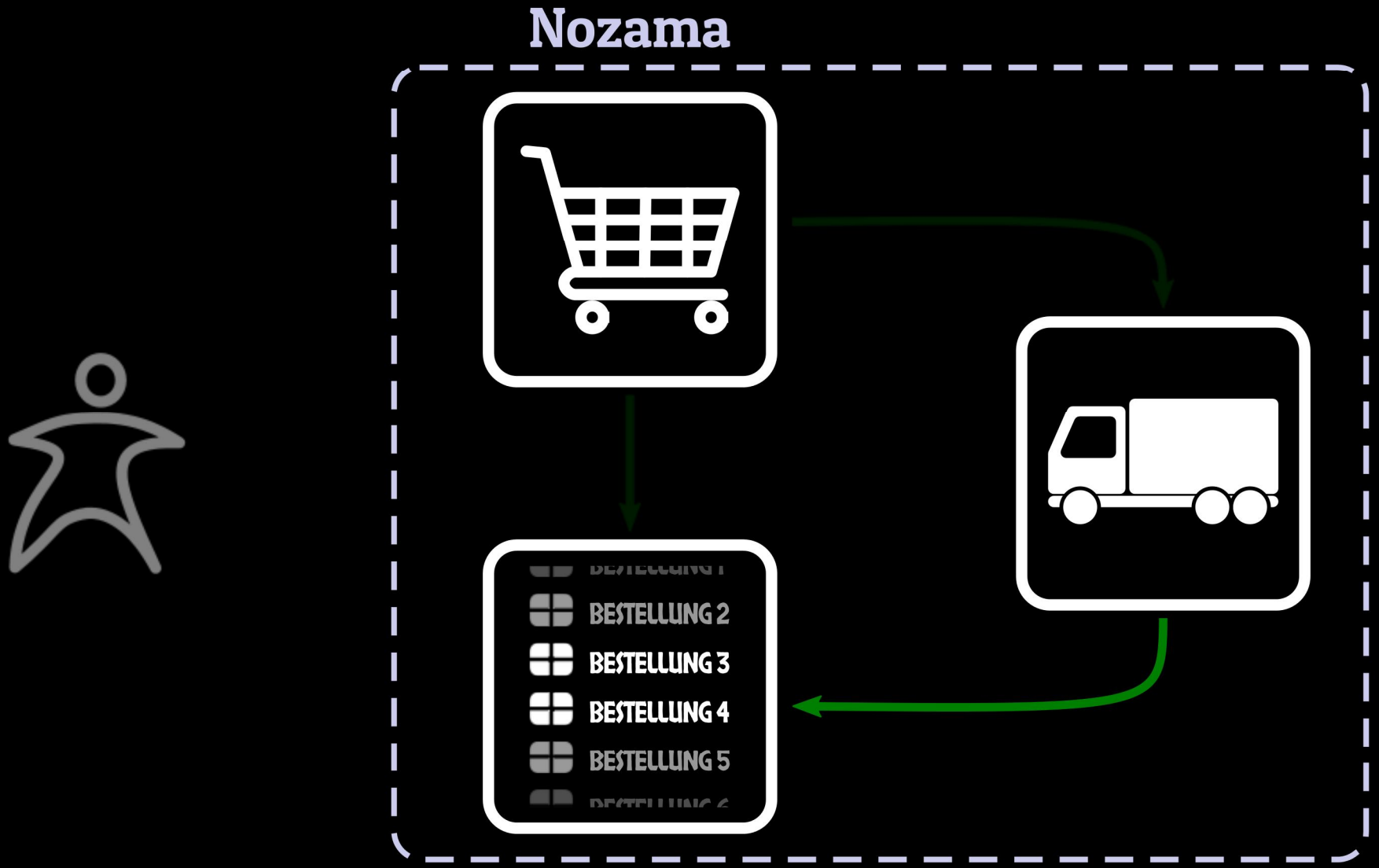
Zonenbasiert



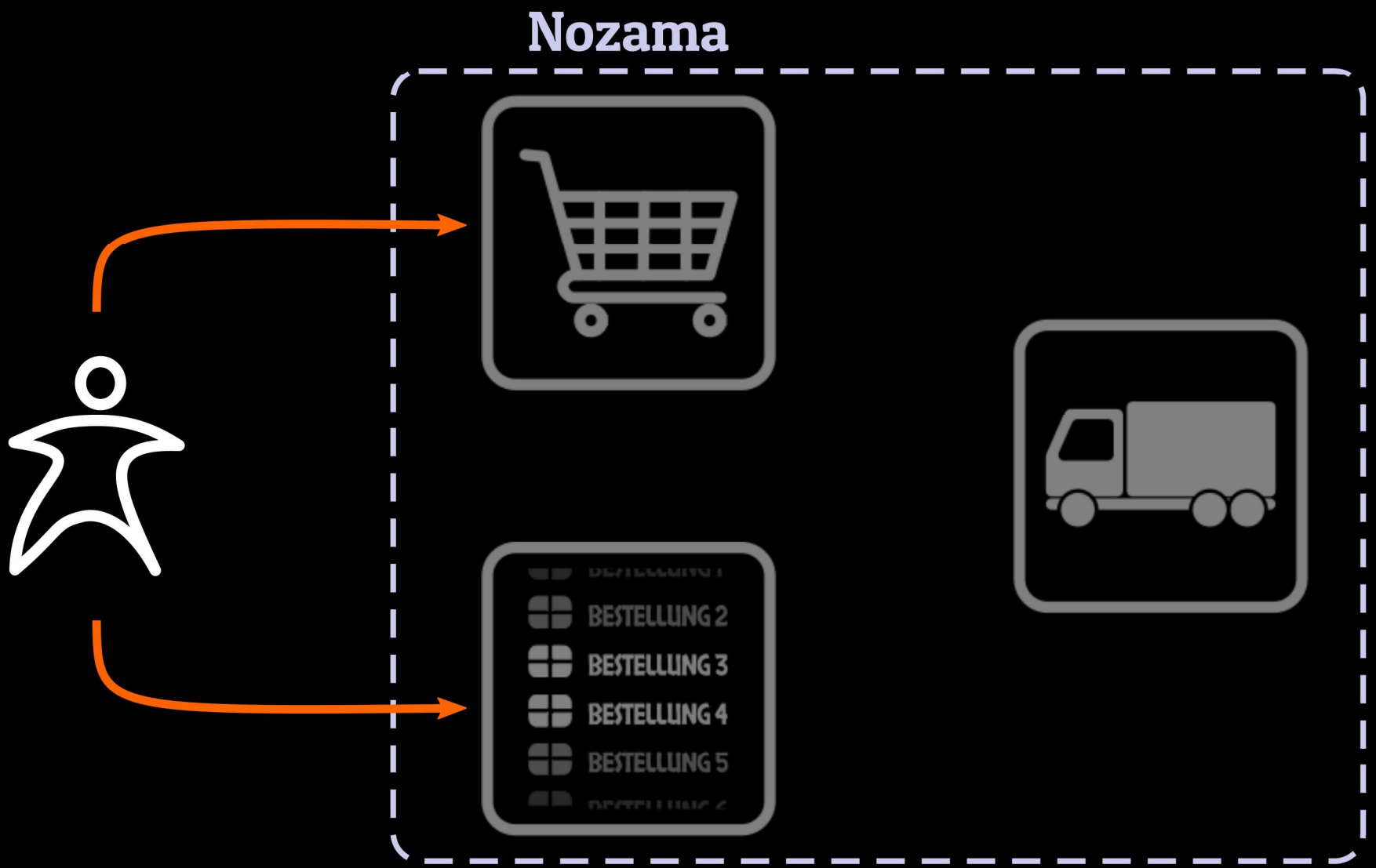
Zonenbasiert



Zonenbasiert

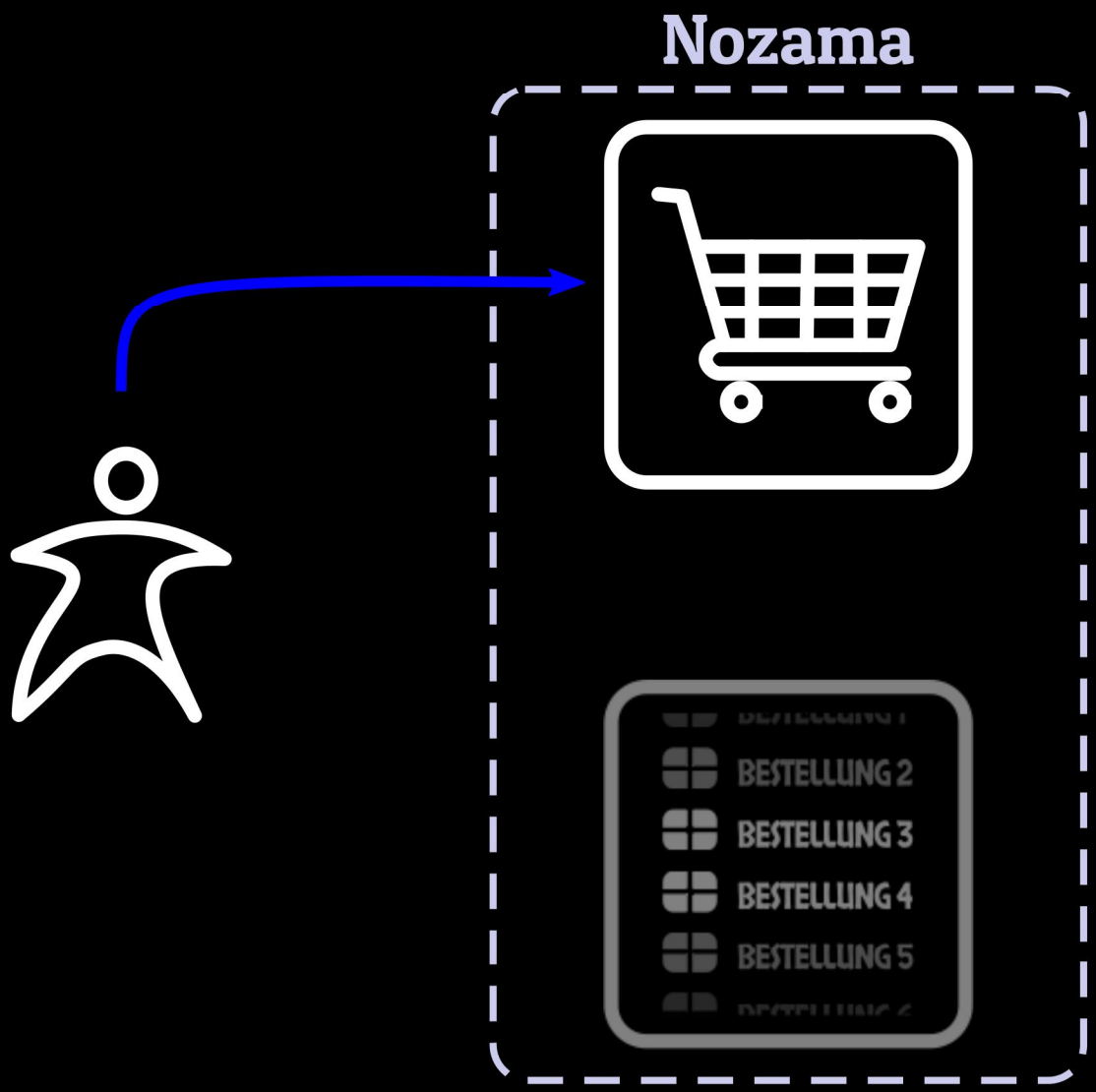


Zonenbasiert

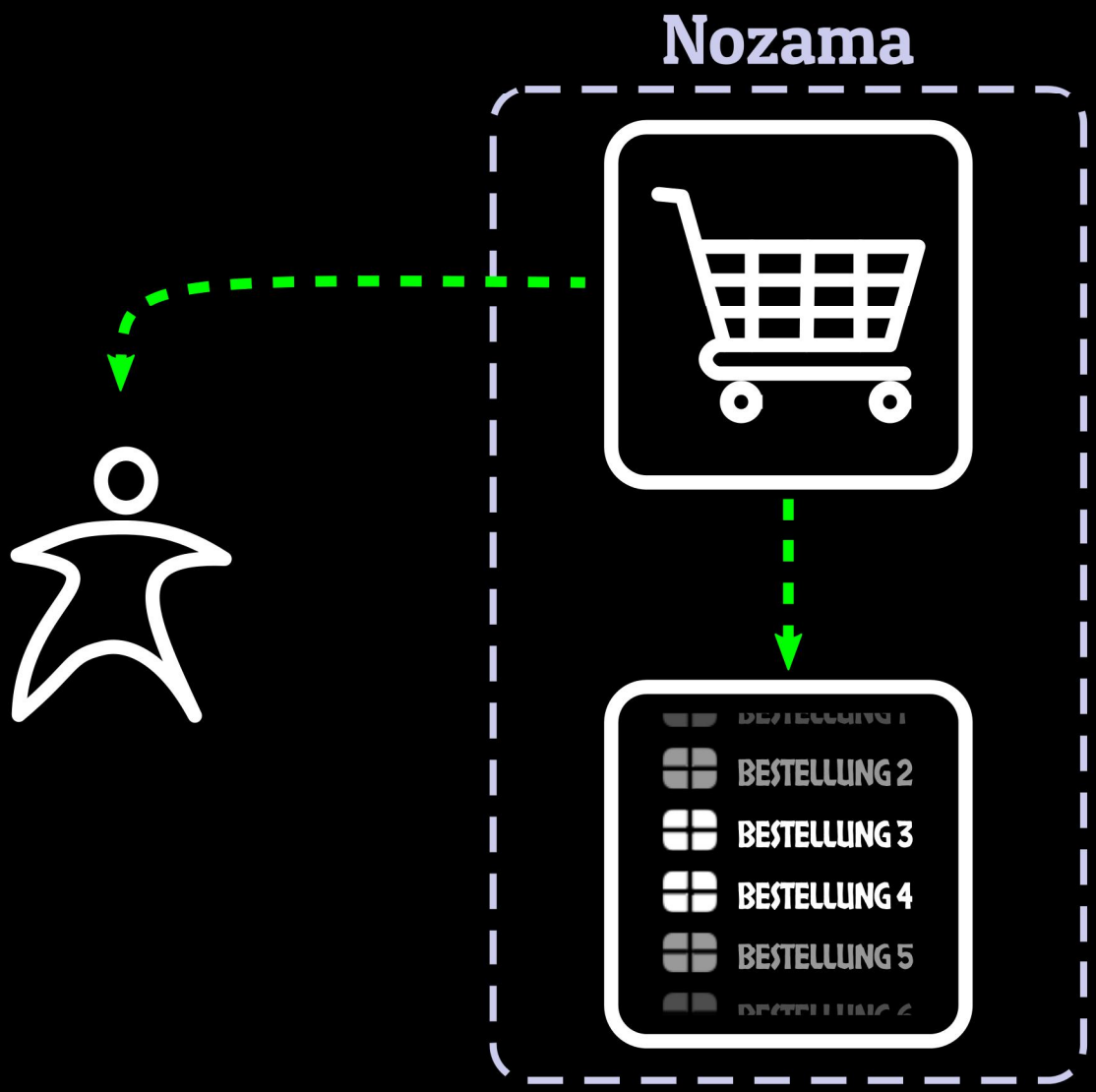


Passwort

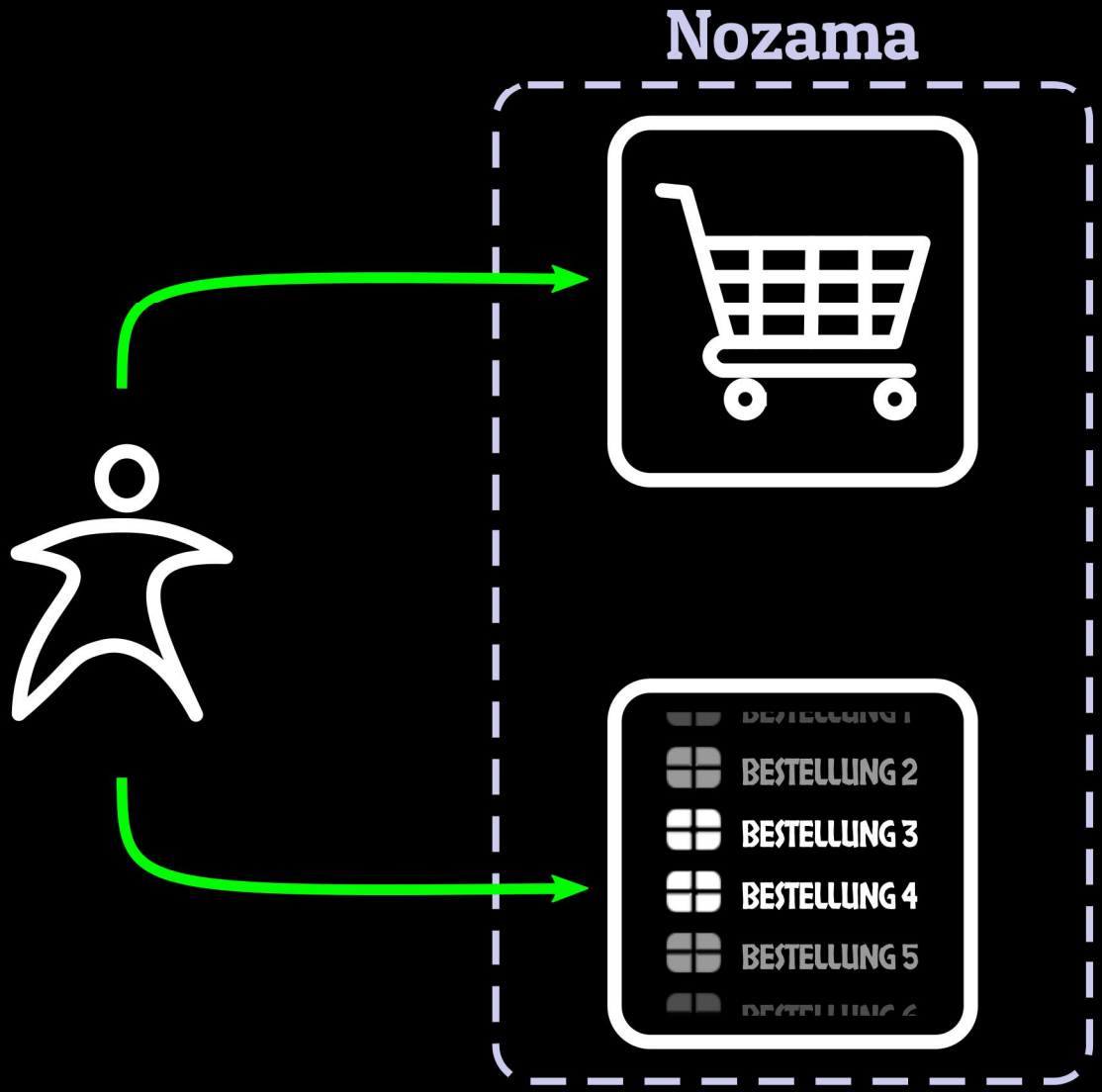
Session


Nozama
BESTELLUNG 2
BESTELLUNG 3
BESTELLUNG 4
BESTELLUNG 5

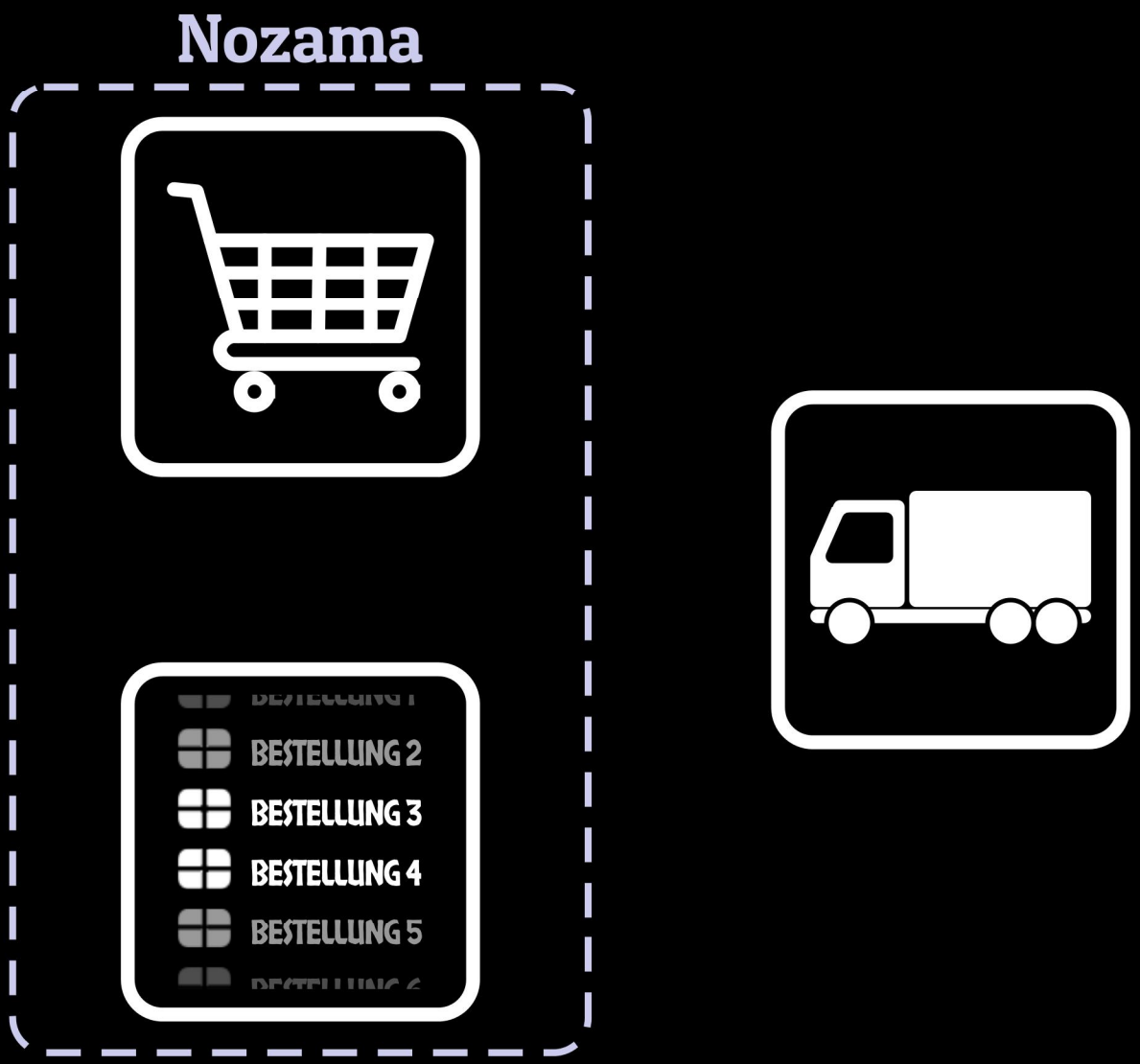
Session


Nozama
BESTELLUNG 2
BESTELLUNG 3
BESTELLUNG 4
BESTELLUNG 5

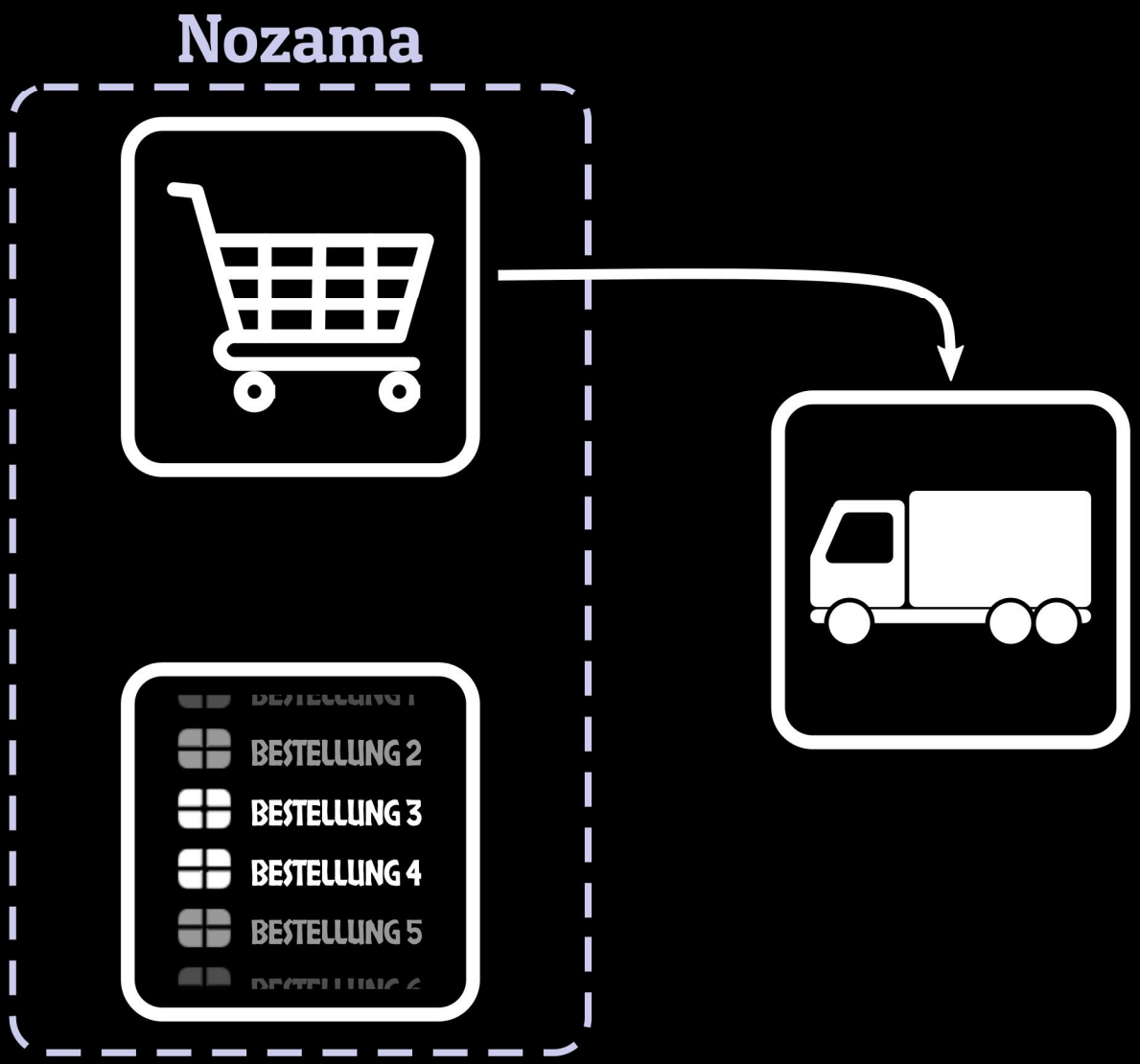
Session


Nozama
BESTELLUNG 2
BESTELLUNG 3
BESTELLUNG 4
BESTELLUNG 5

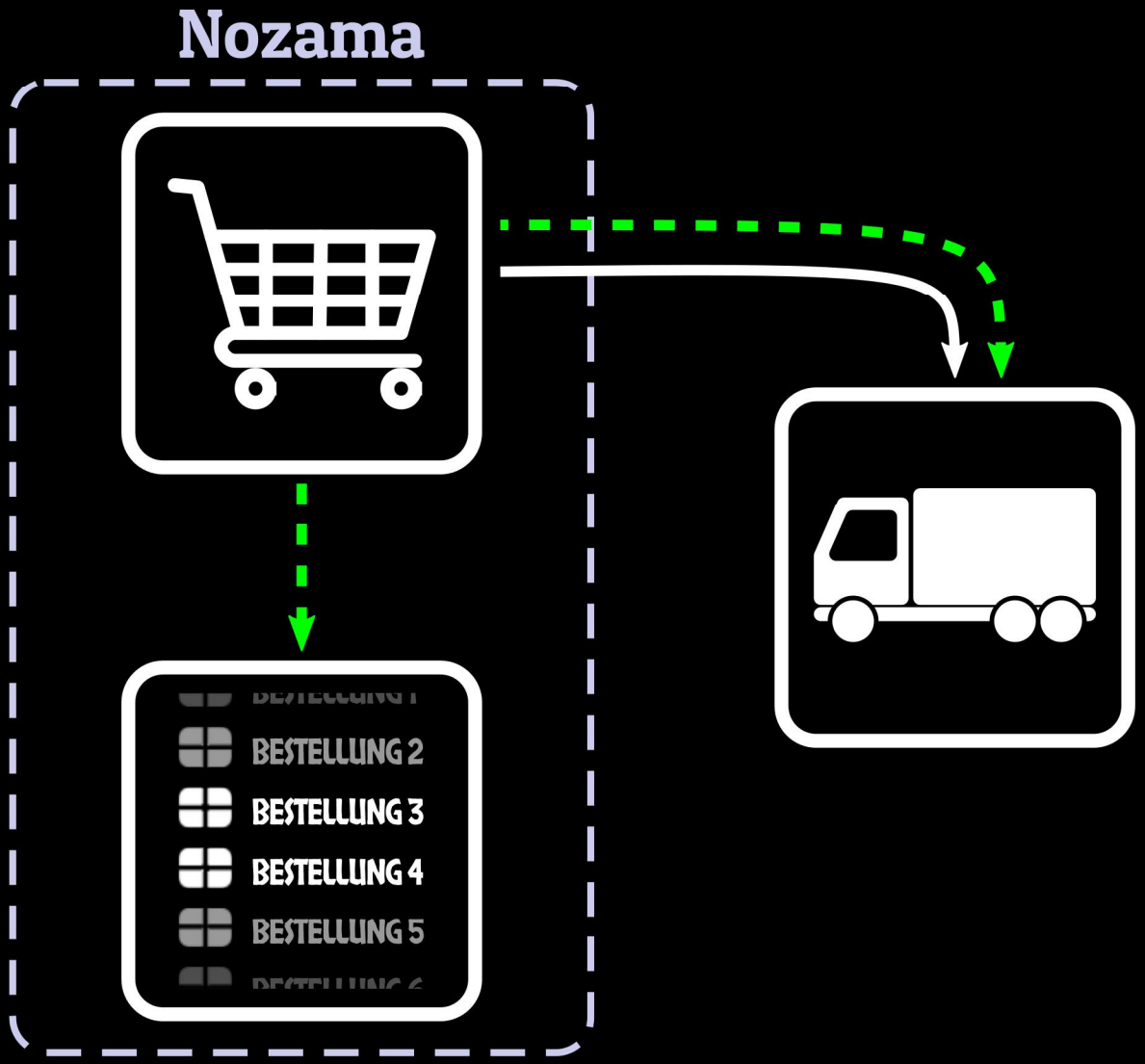
One-time password



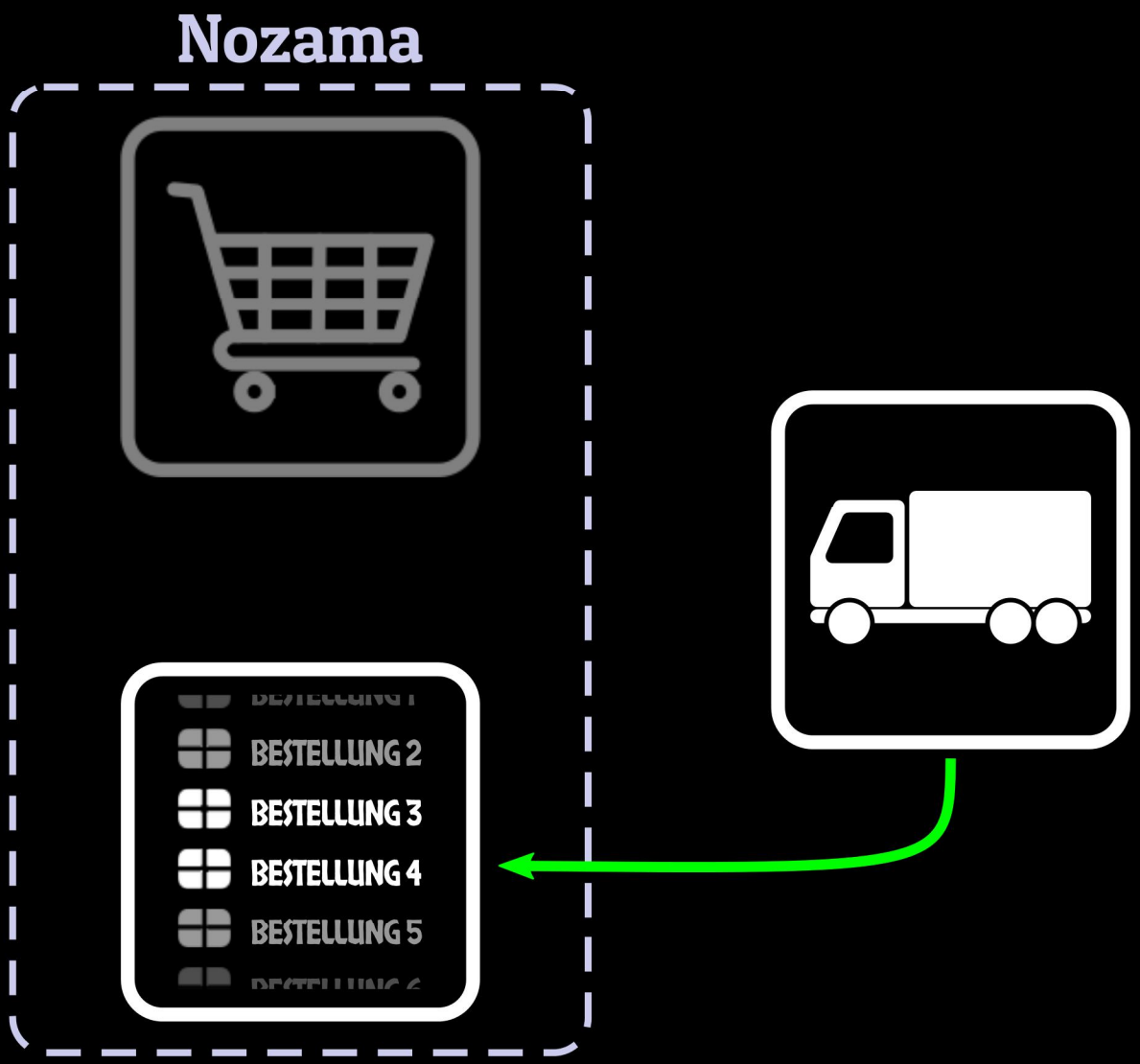
One-time password



One-time password

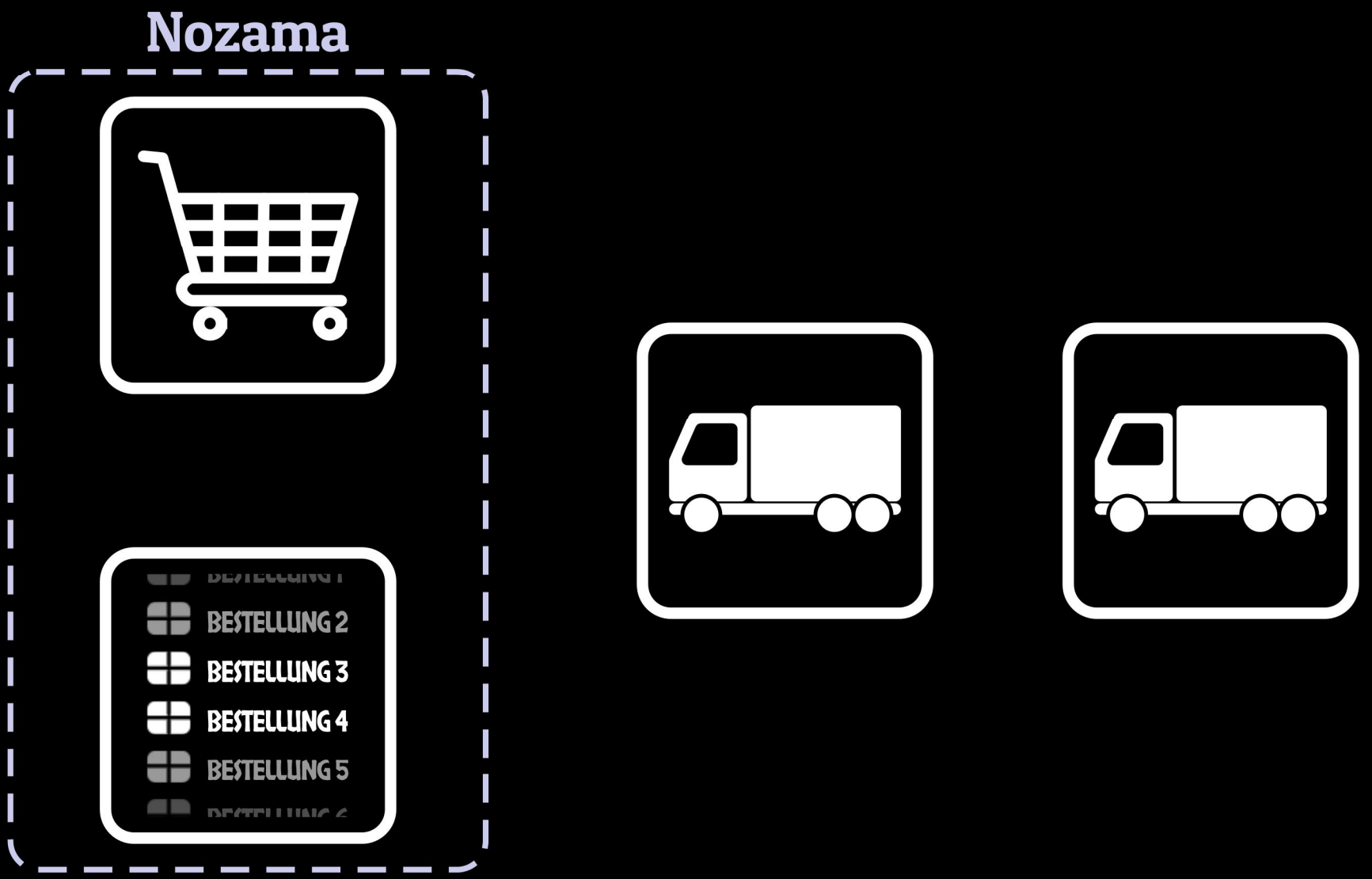


One-time password

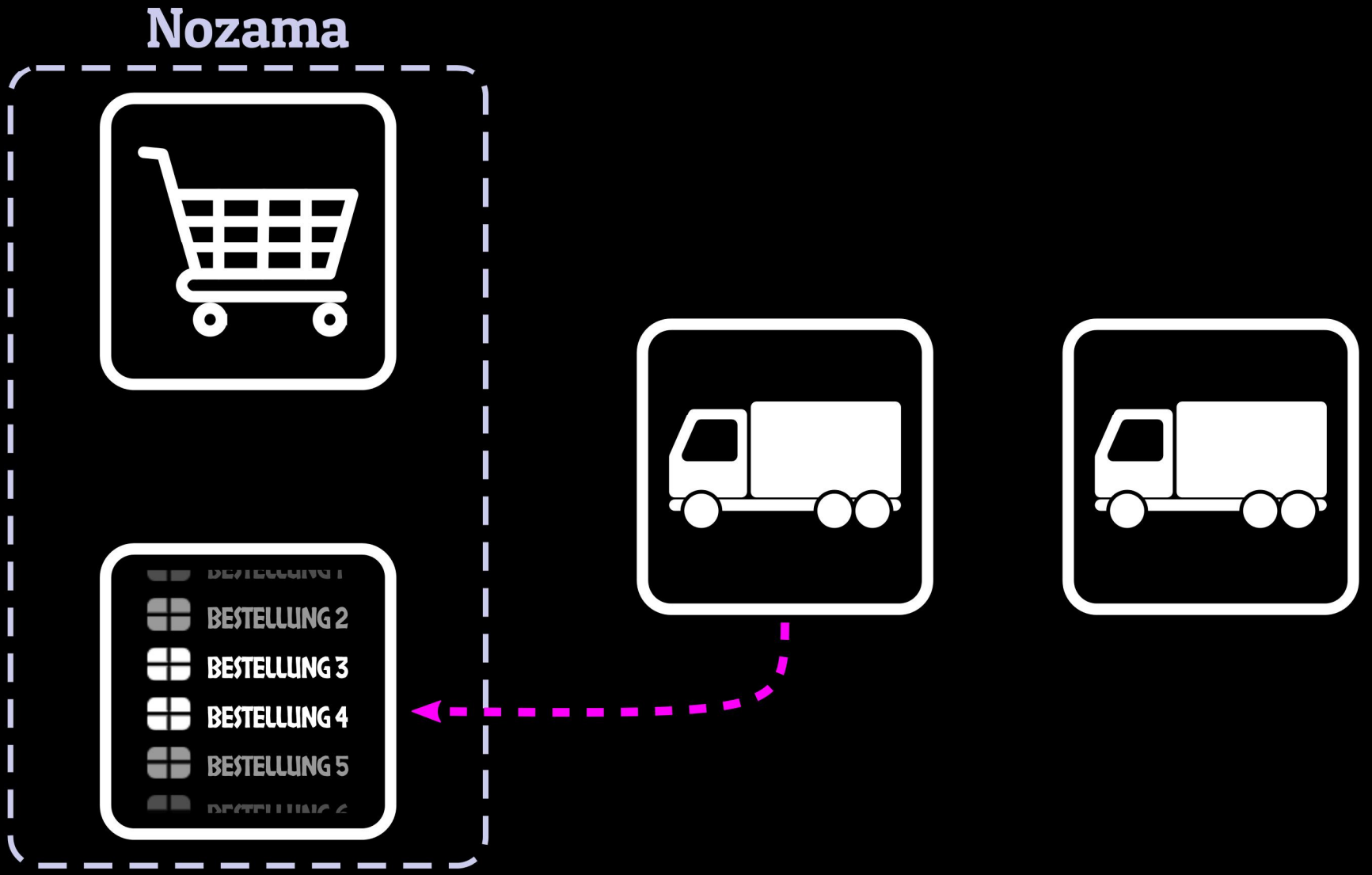


Peer to Peer

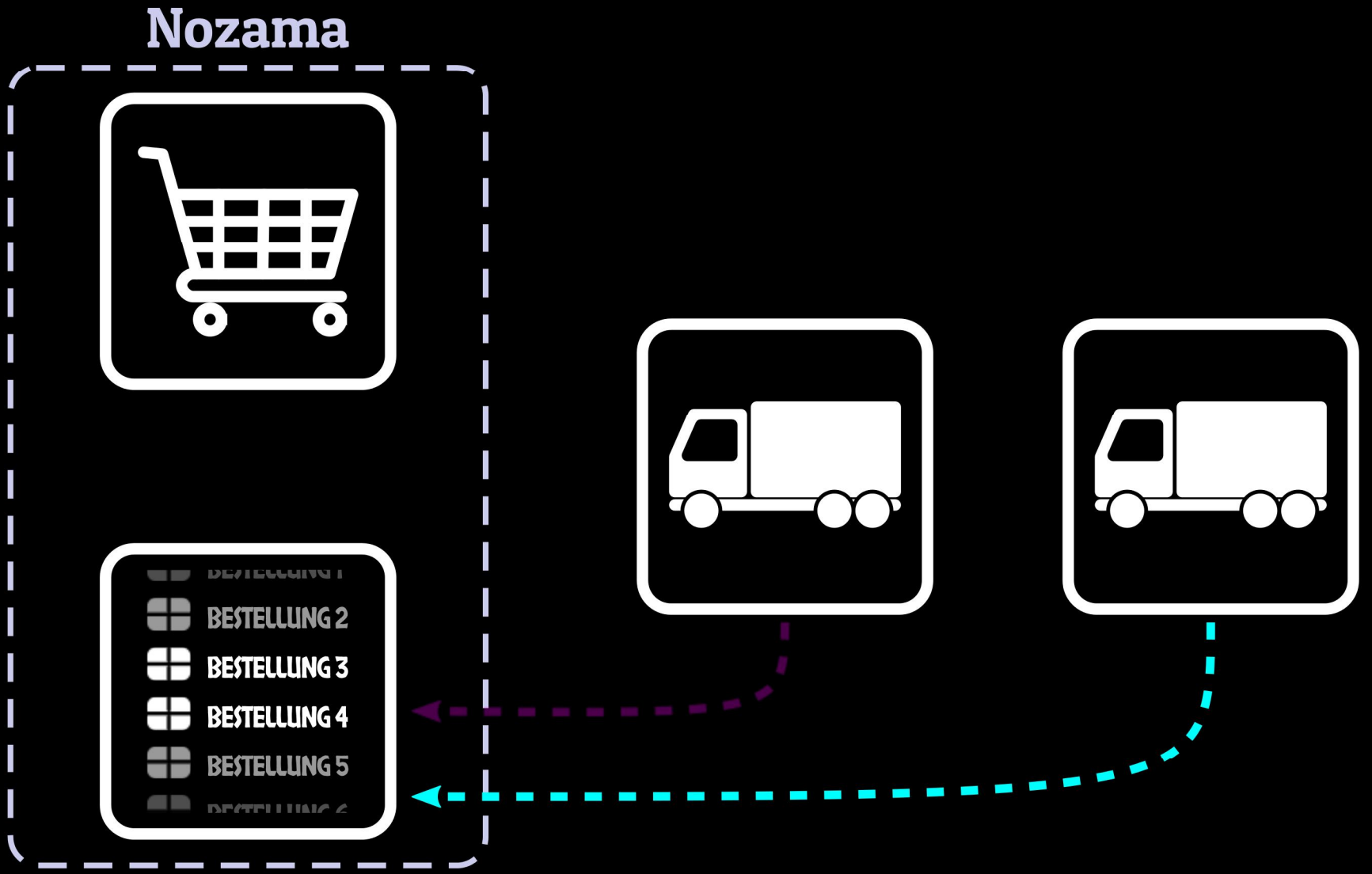
Peer to Peer


Nozama
BESTELLUNG 2
BESTELLUNG 3
BESTELLUNG 4
BESTELLUNG 5

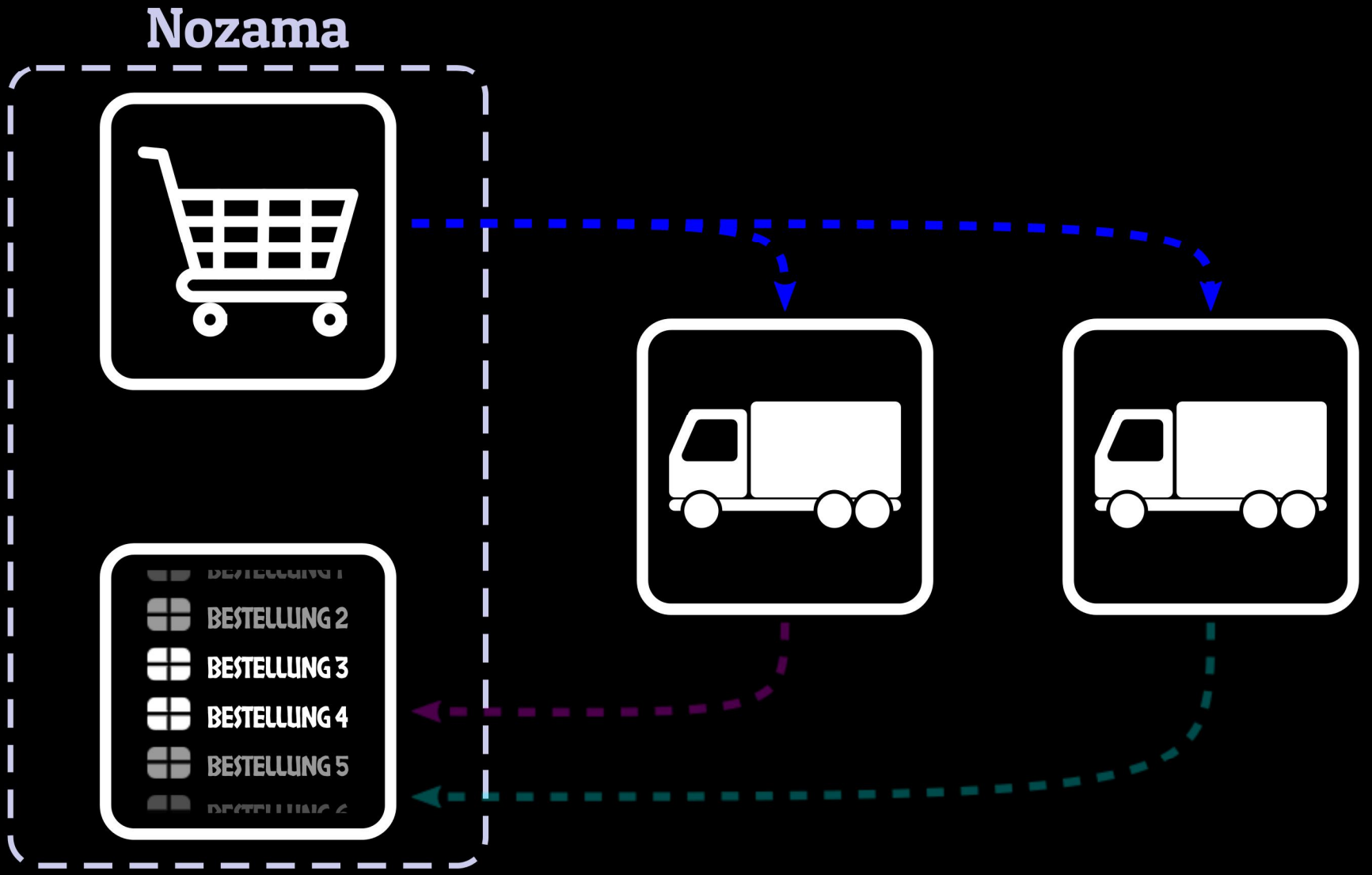
Peer to Peer


Nozama
BESTELLUNG 2
BESTELLUNG 3
BESTELLUNG 4
BESTELLUNG 5

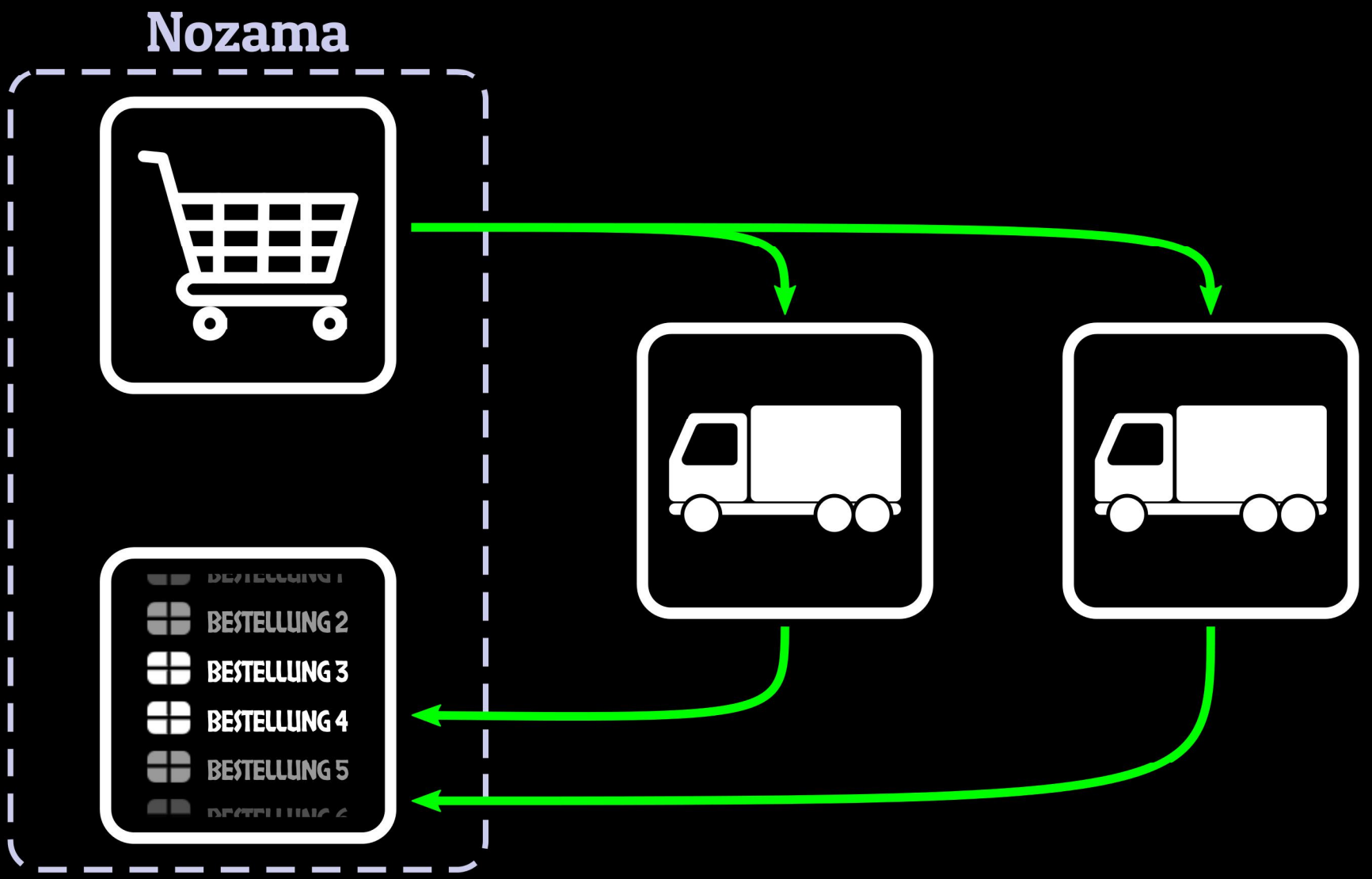
Peer to Peer


Nozama
BESTELLUNG 2
BESTELLUNG 3
BESTELLUNG 4
BESTELLUNG 5

Peer to Peer

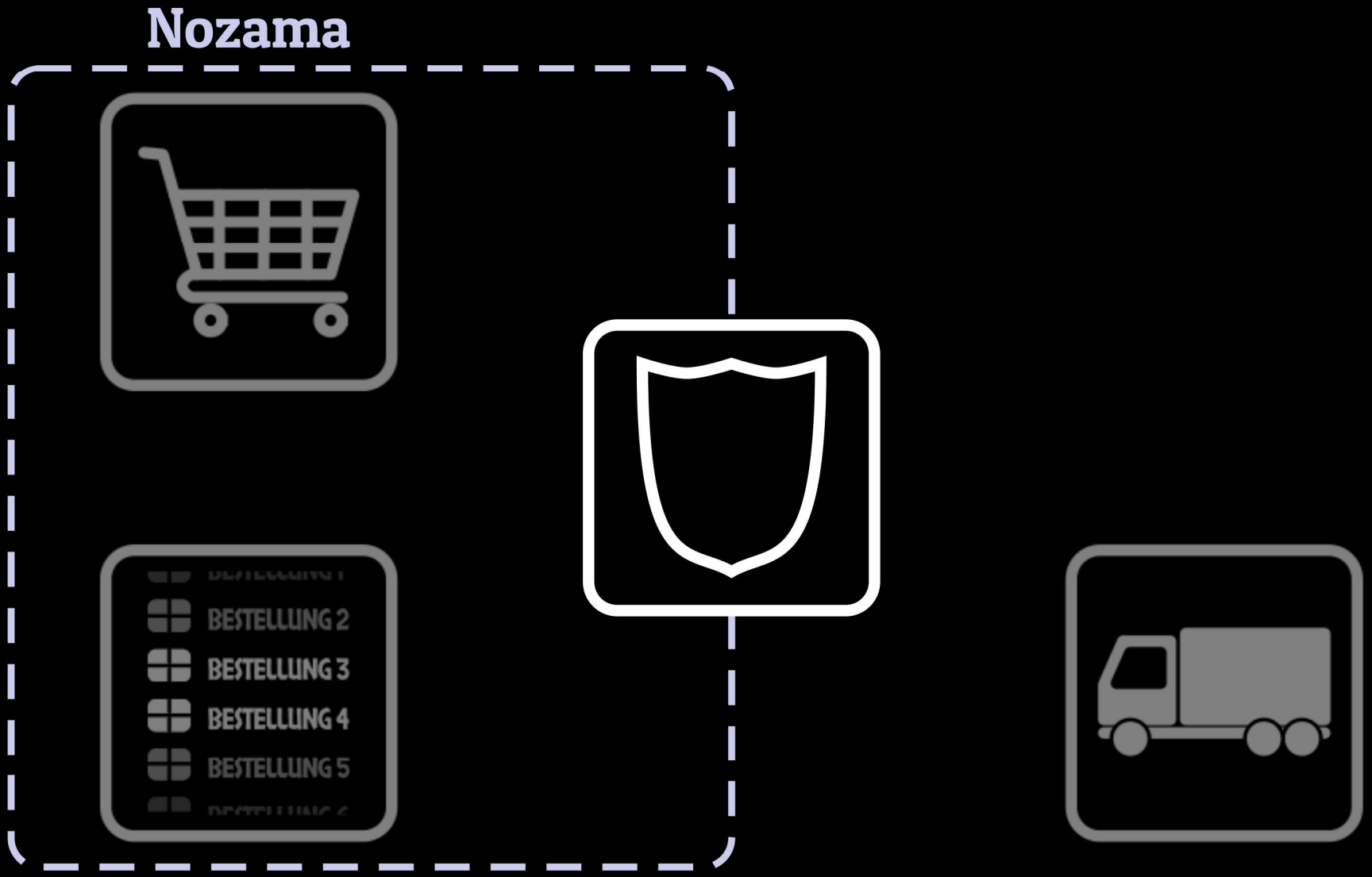

Nozama
BESTELLUNG 2
BESTELLUNG 3
BESTELLUNG 4
BESTELLUNG 5

Peer to Peer

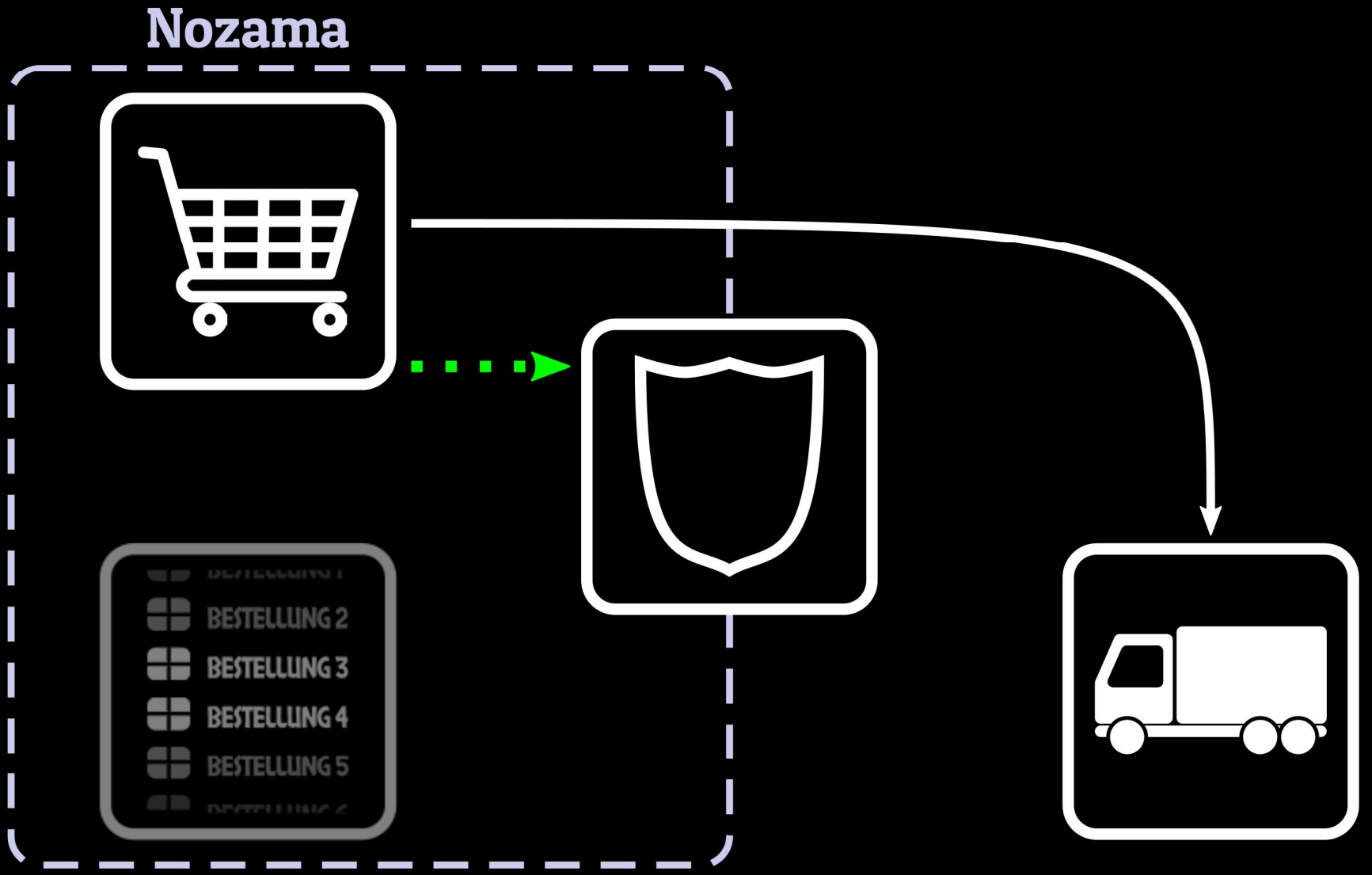

Nozama
BESTELLUNG 2
BESTELLUNG 3
BESTELLUNG 4
BESTELLUNG 5

zentrale Zugriffskontrolle

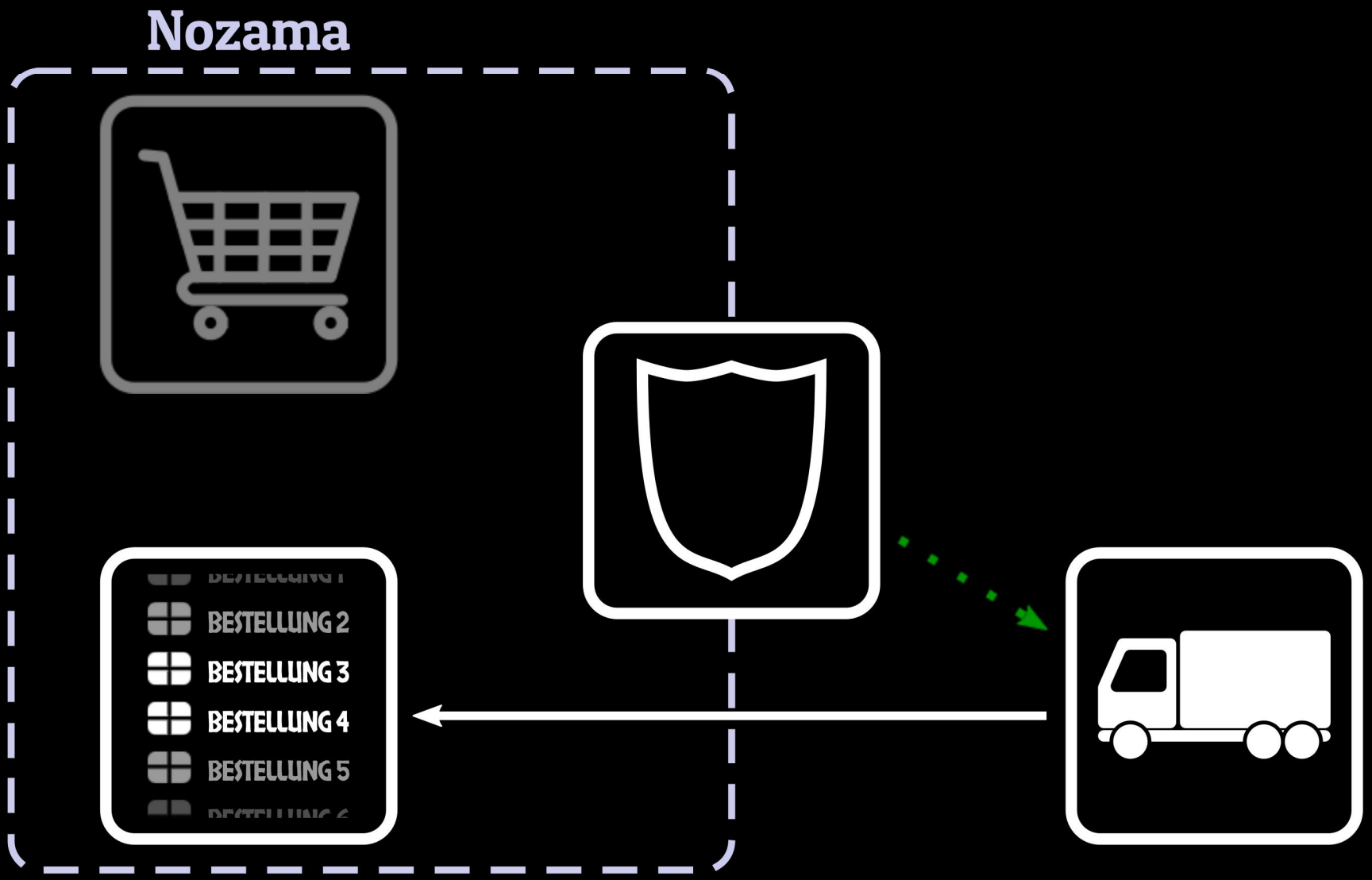
zentrale Zugriffskontrolle



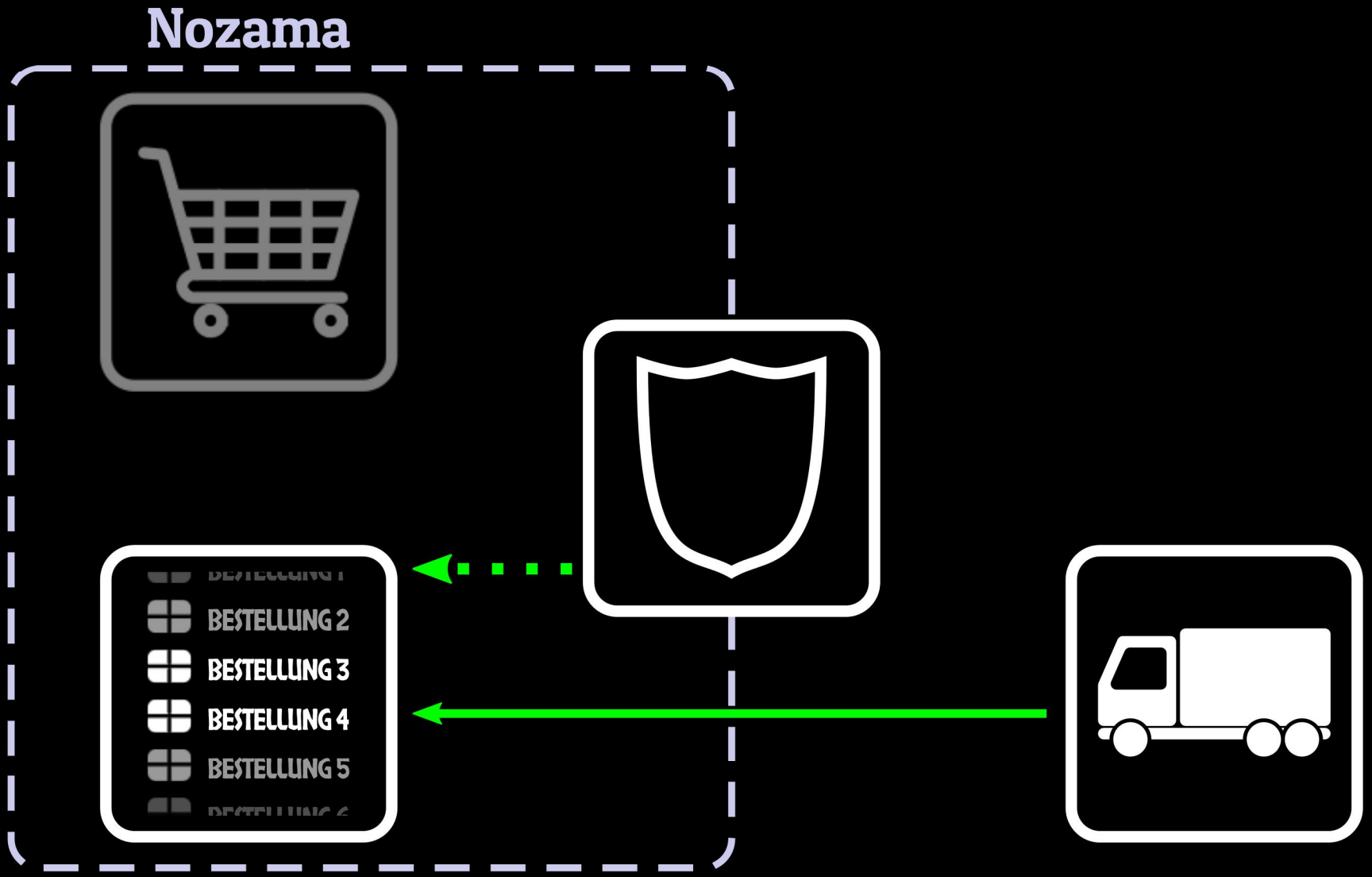
zentrale Zugriffskontrolle



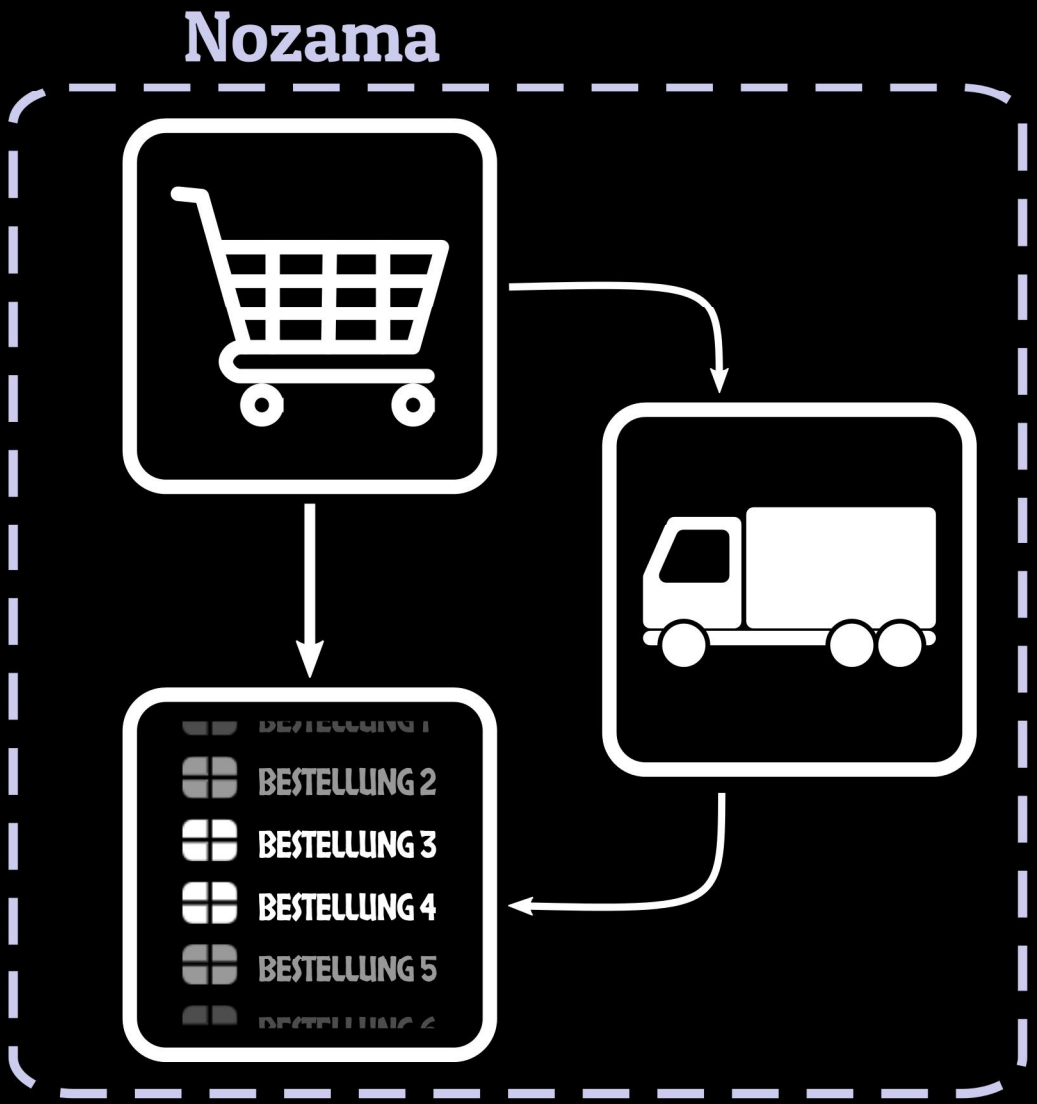
zentrale Zugriffskontrolle

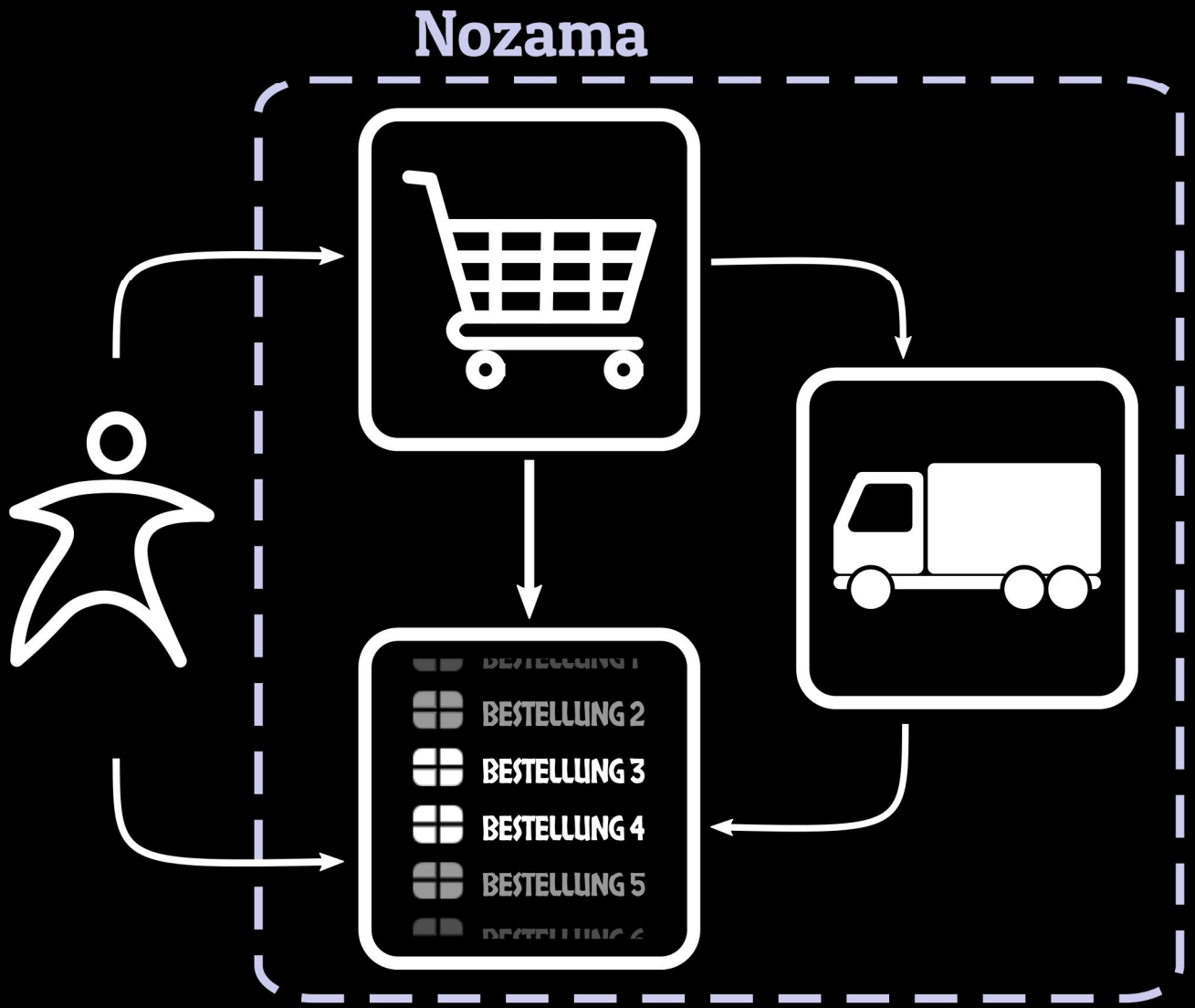


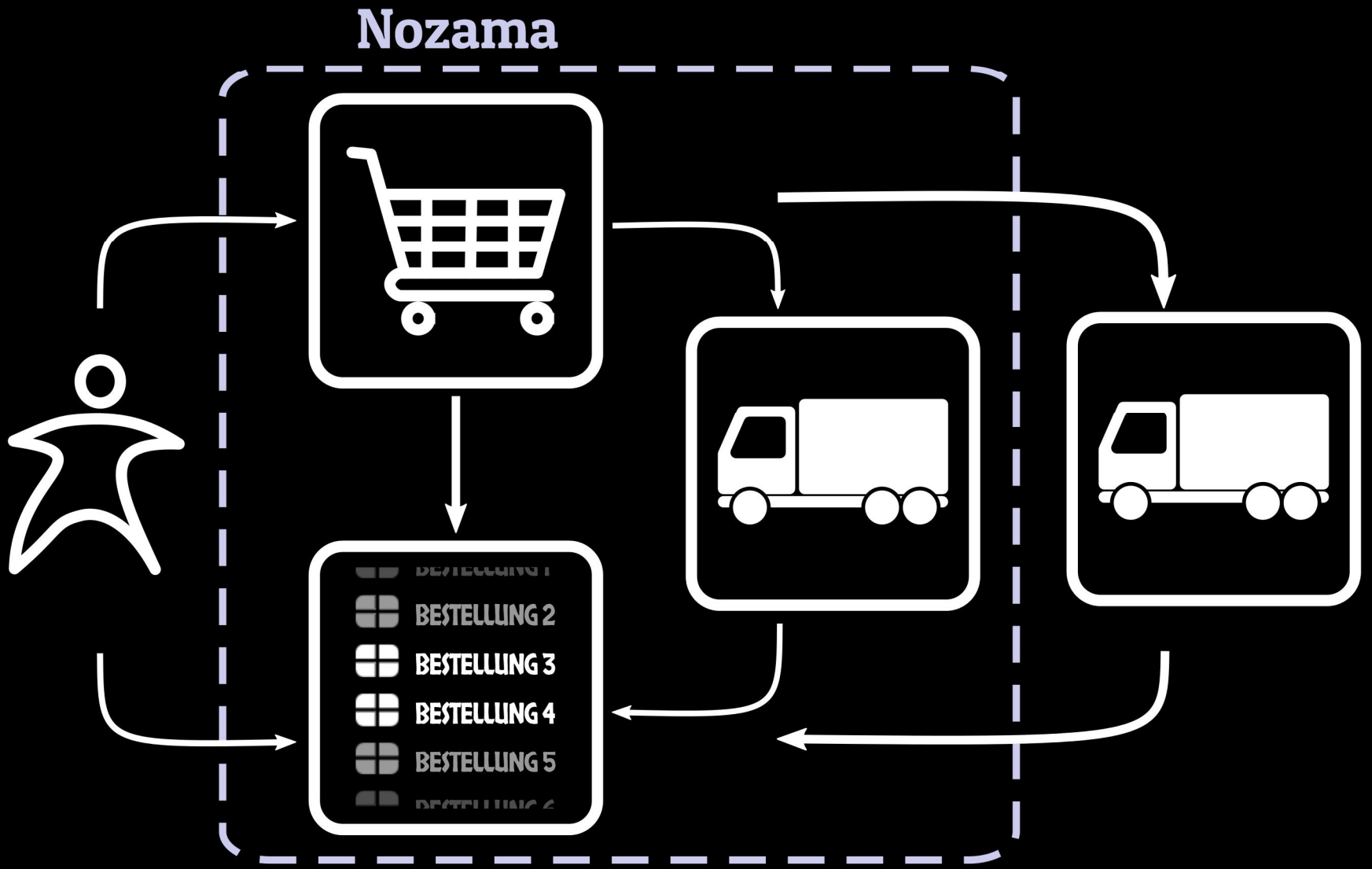
zentrale Zugriffskontrolle

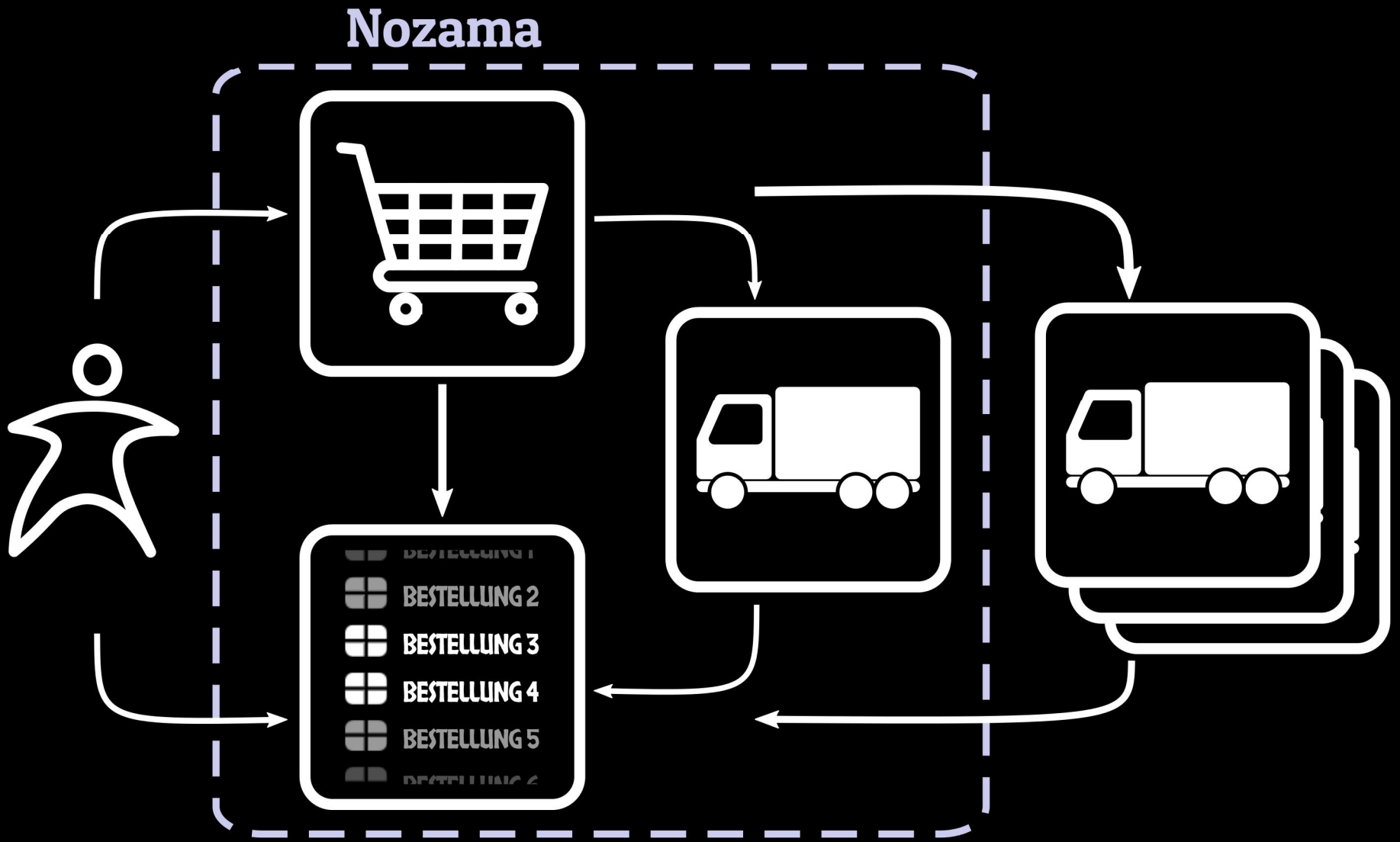


no silver bullet


Nozama
BESTELLING 2
BESTELLING 3
BESTELLING 4
BESTELLING 5


Nozama
BESTELLING 2
BESTELLING 3
BESTELLING 4
BESTELLING 5


Nozama
BESTELLING 2
BESTELLING 3
BESTELLING 4
BESTELLING 5


Nozama
BESTELLING 2
BESTELLING 3
BESTELLING 4
BESTELLING 5

Token!

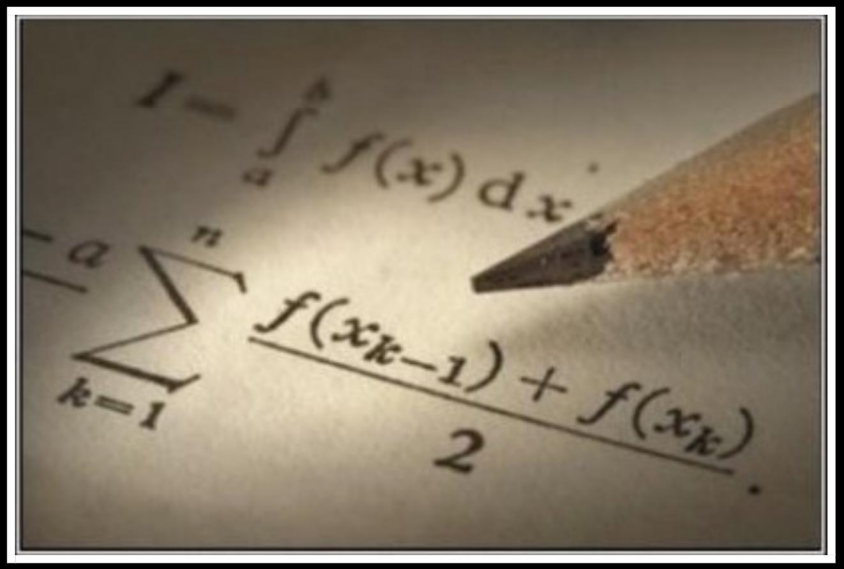
Was sind Token?

```
   Payload
+ Signatur
----------
=     Token
```

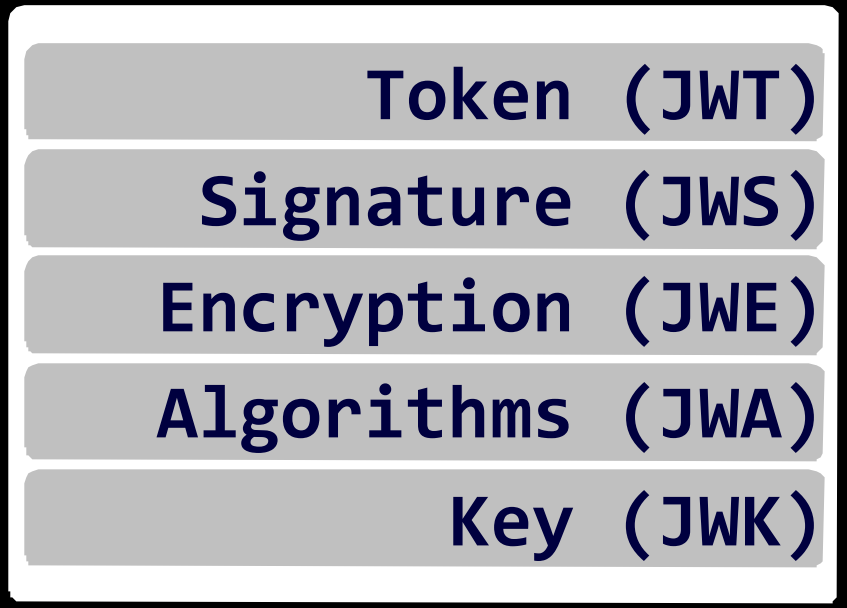
Fahrkarte als digitales Token

Payload	2 Stunden, bis 18:00Uhr
Signatur	badc0ded
Token	MiBTdHVuZGVuLCBiaXMgMTg6MDBVaHJ8YmFkYzBkZWQNCg==

Signatur-Verfahren



JSON Web Token


Token (JWT)
Signature (JWS)
Encryption (JWE)
Algorithms (JWA)
Key (JWK)

JSON Web Signature & Token

```
eyJhbGciOiJIUzI1NiIsI
nR5cCI6IkpXVCJ9.eyJzd
WIiOiJNaWNyb3hjaGcyMD
E1IiwibmFtZSI6Ik1hcnR
pbiIsInNwZWFrZXIiOnRy
dWV9.4x3Q9eMUHi5UY0cD
kkvjhr1le4kbpWeXRn2WP
wEV-9E
```

JWS

```
{ "alg": "HS256",
  "typ": "JWT"}
```

Header

```
{    "sub": "Microxchg2015",
   "name": "Martin",
"speaker": true }
```

JWT

```
HMACSHA256(
 base64Url(header) + "." +
 base64Url(payload),
 "a_strong_secret")
```

Pseudocode

JWS mit Private Key

```
eyJpc3MiOiJtaWNyb3hja
GciLCJhbGciOiJSUzI1Ni
J9.eyJzdWIiOiJtYXJ0aW
4iLCJleHAiOjE0MjM2MTA
0NDB9.jckJWw780QcW0nD
8ngz44SYmYFUuWYg9UWxS
fnT7ofOuuP2-kTm-PEmta
zXllOg0sR22gMPIg69VzP
1rIOXHZl45IL_udIh71nO
staqaLOCnG_CduKFiGjgX
2jdfu6tcF_AKiWrVQeqAs
XpN0tfgoN21SOSlv_P229
SZtwItpf4
```

JWS

```
{
  "alg": "RS256"
  "typ": "JWT",
}
```

Header

```
{
  "sub": "martin",
  "exp": 1423610440
}
```

JWT

```
RSA(
  HMACSHA256(...),
  privateKey)
)
```

Pseudocode

Macaroons

Macaroons

```
MDAxYWxvY2F0aW9uIG1pY
3JveGNoZy5pbwowMDFkaW
RlbnRpZmllciBNaWNyb3h
jaGcyMDE1CjAwMTRjaWQg
bmFtZT1NYXJ0aW4KMDAxN
WNpZCBzcGVha2VyPXRydW
UKMDAyZnNpZ25hdHVyZSC
Jll9kCL-ftb6GU791D3bX
eE-FbdIG3Uj154dCiaB6c
go
```

Serialized Macaroon

```
location microxchg.io
identifier Microxchg2015
cid name=Martin
cid speaker=true
```

Identifier & Caveats

```
HMACSHA256(payload,
 "a_strong_secret")
```

Pseudocode

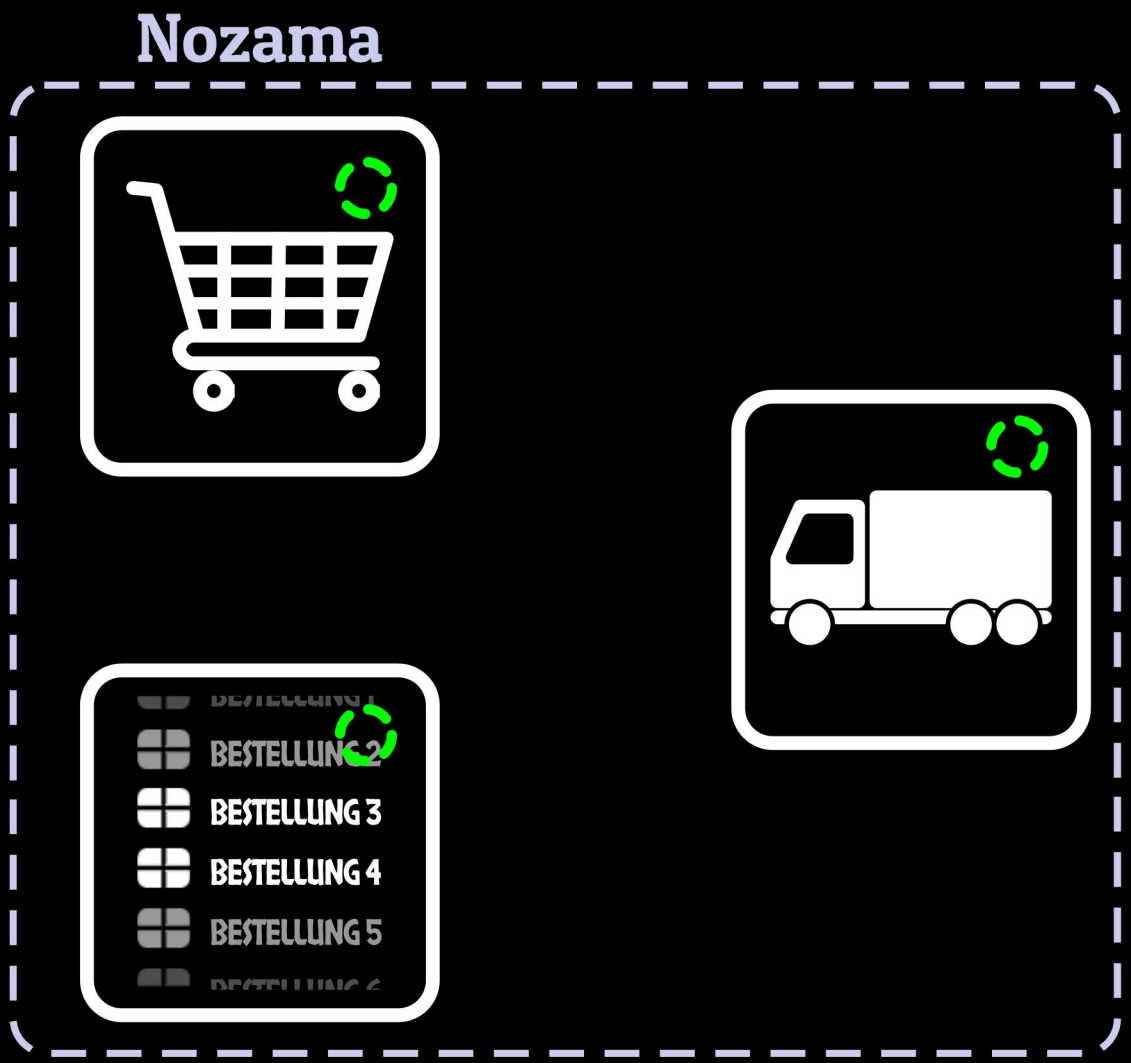
Flexibilität

SWT? Macaroons? JWT?

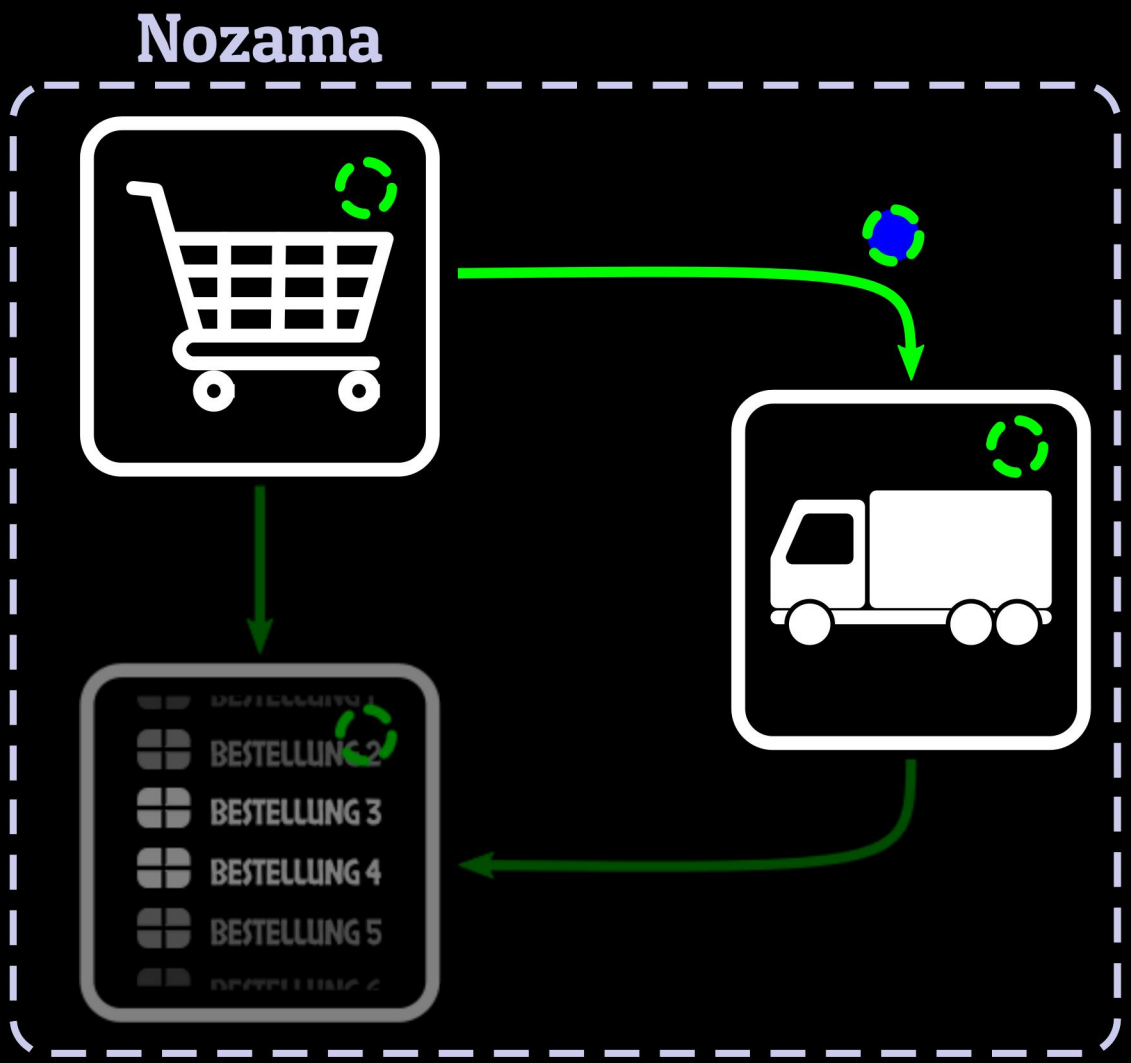
Und in der Praxis

Zonenbasiert

Zonenbasiert

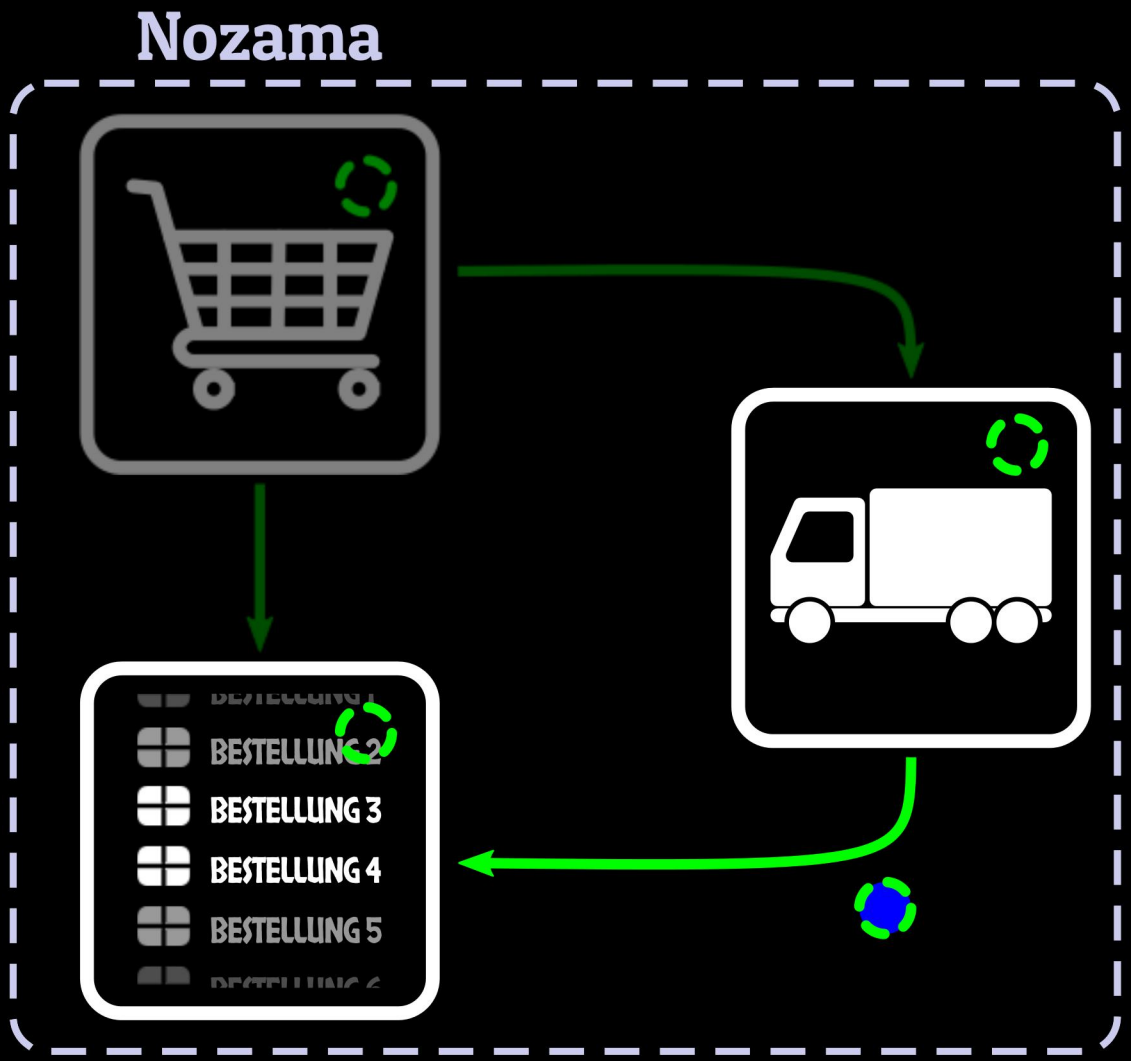


Zonenbasiert



Token	
challenge	grb4g3
expires:	now+5s
signed:	nozama

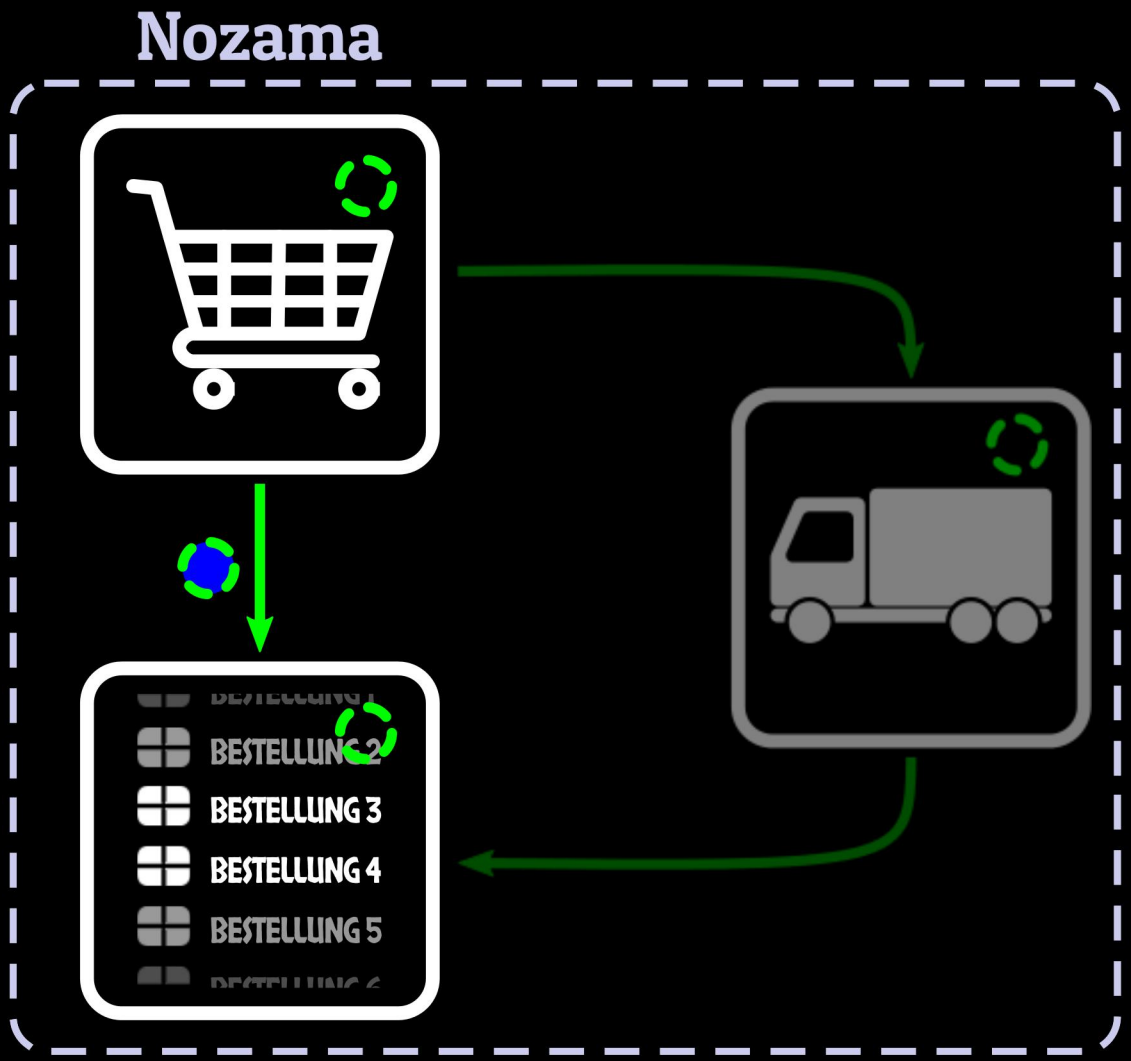
Zonenbasiert



Token

challenge	tr4sh
expires:	now+5s
signed:	nozama

Zonenbasiert

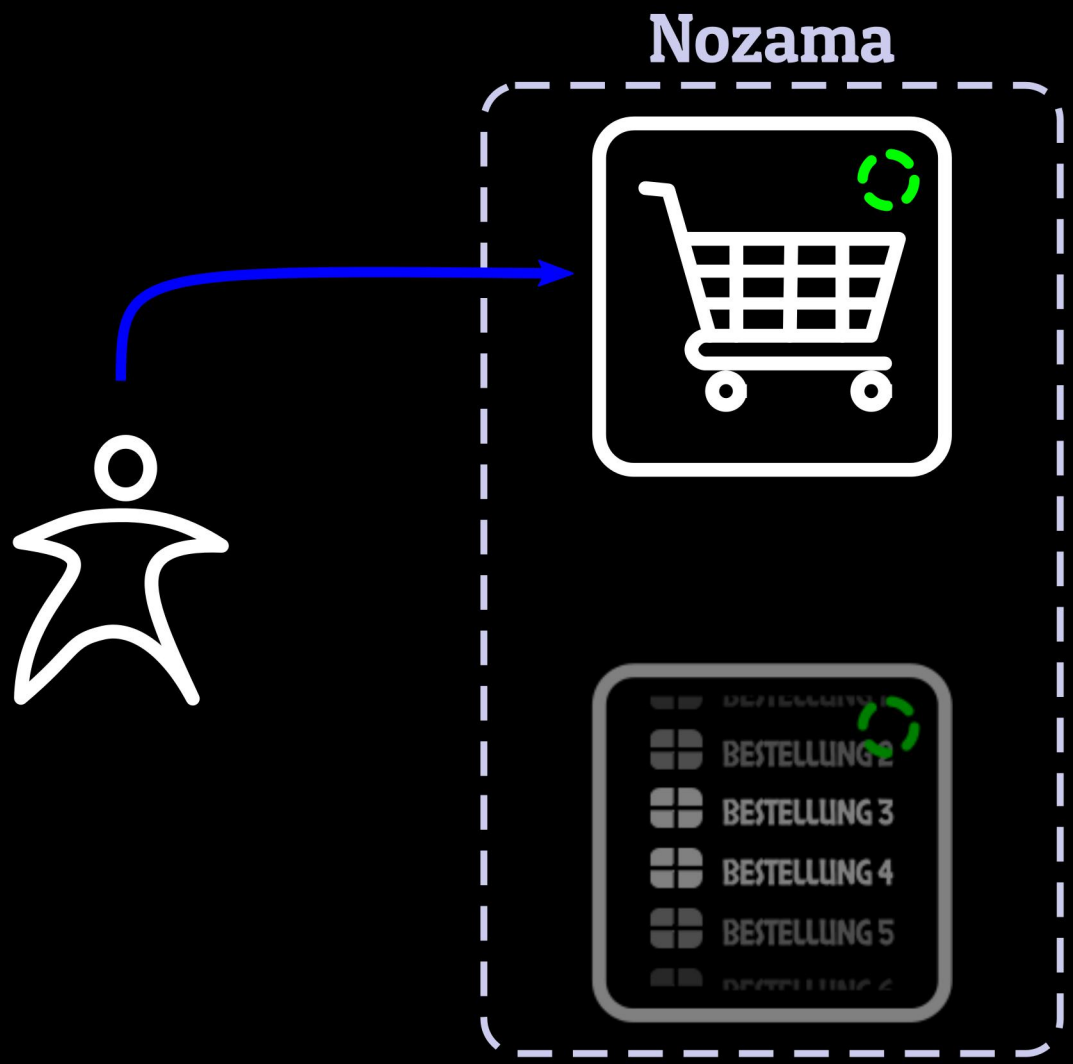


Token

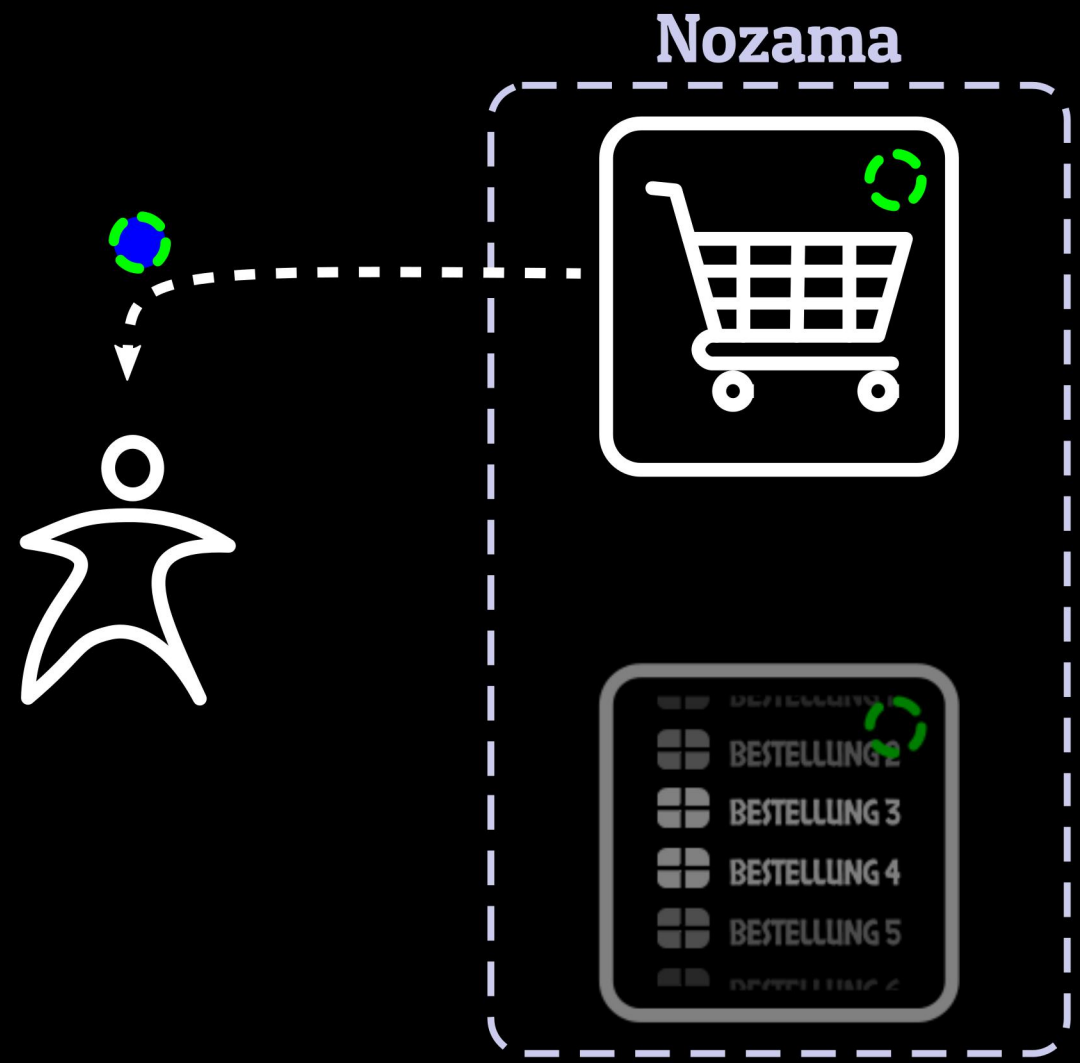
challenge	w4st3
expires:	now+5s
signed:	nozama

Session

Session



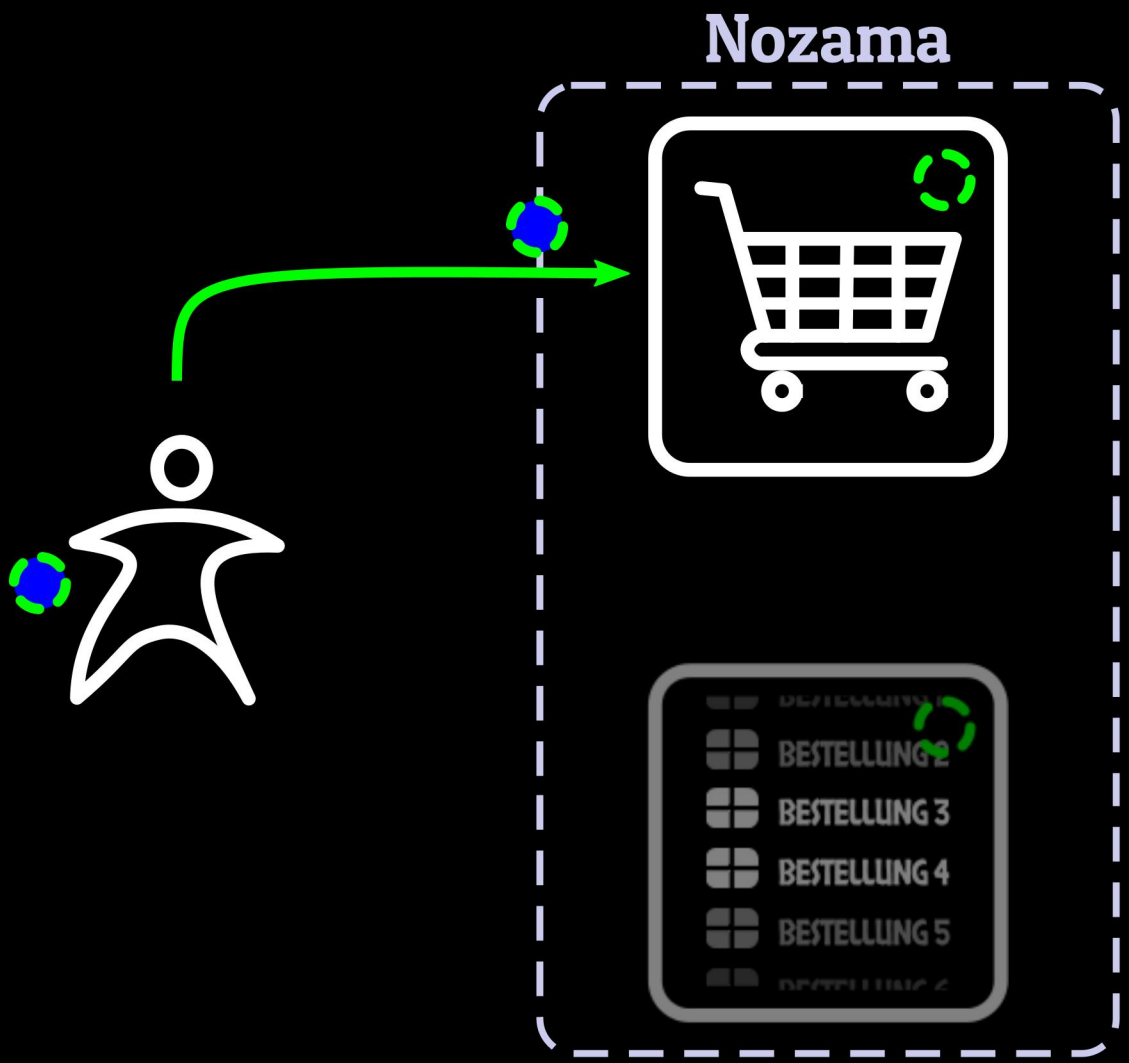
Session



Token

username:	john
userid:	pagd42
vip:	true
expires:	15:20
signed:	nozama

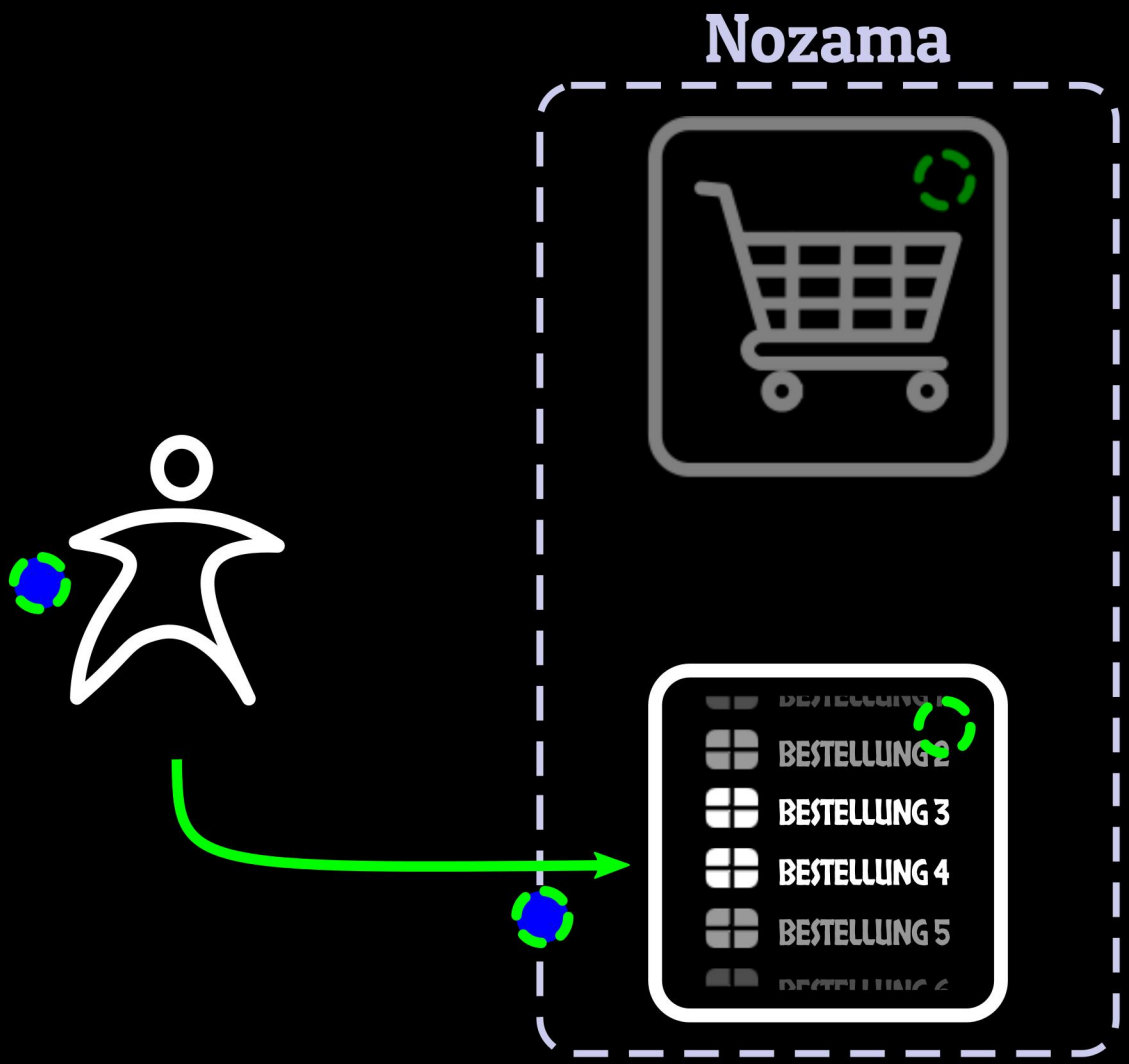
Session



Token

username:	john
userid:	pagd42
vip:	true
expires:	15:20
signed:	nozama

Session

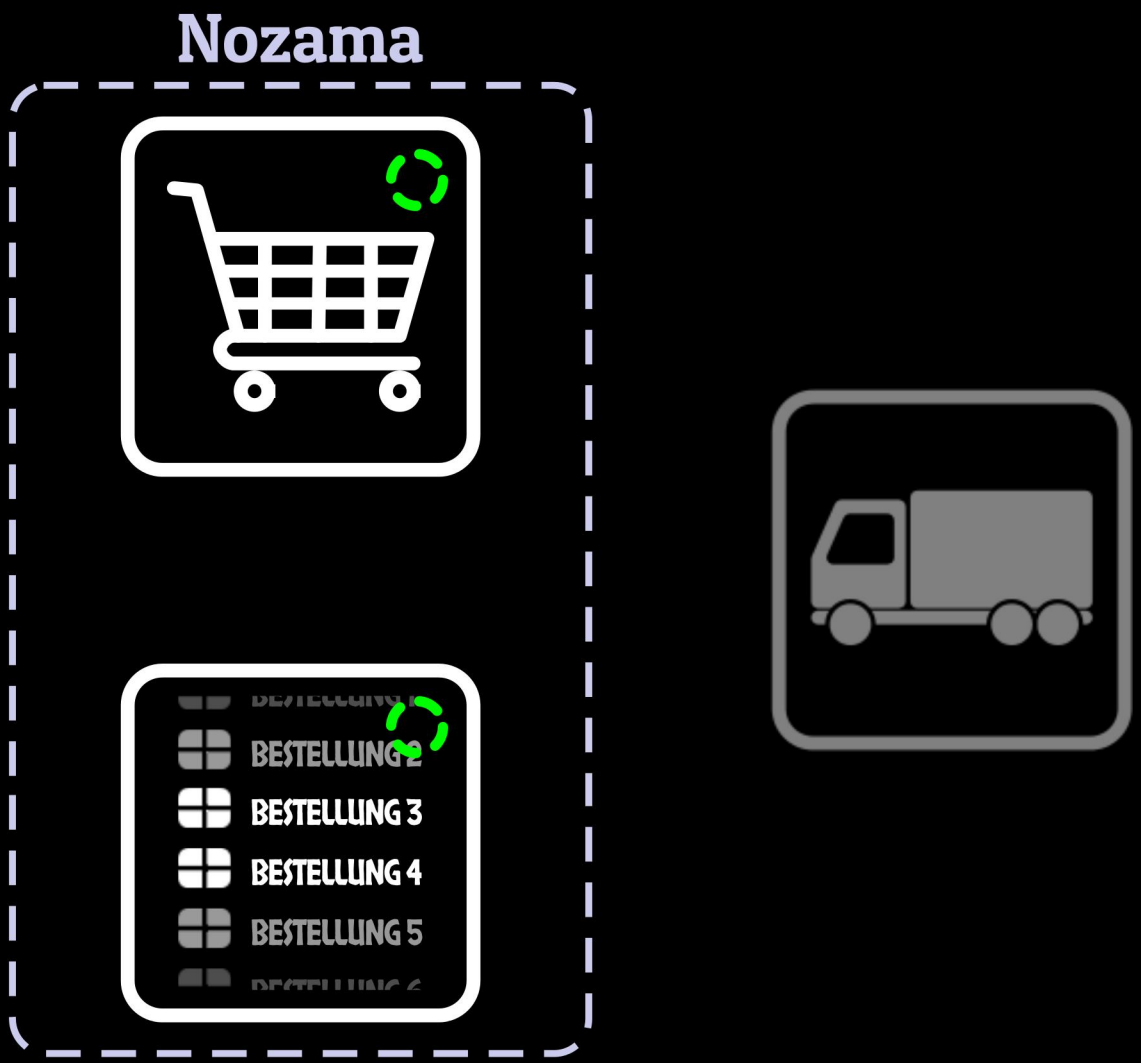


Token

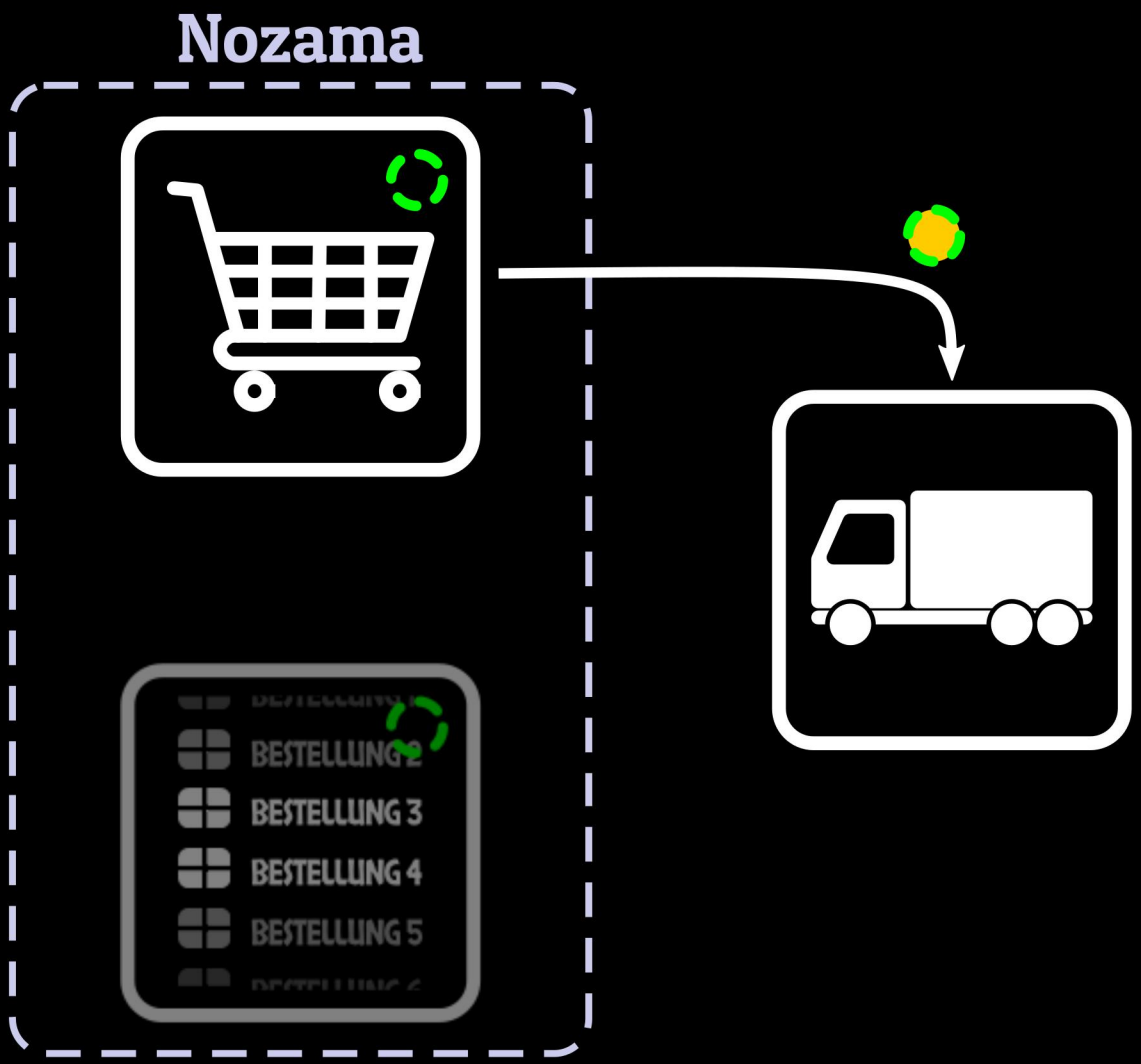
username:	john
userid:	pagd42
vip:	true
expires:	15:20
signed:	nozama

One-time password

One-time password



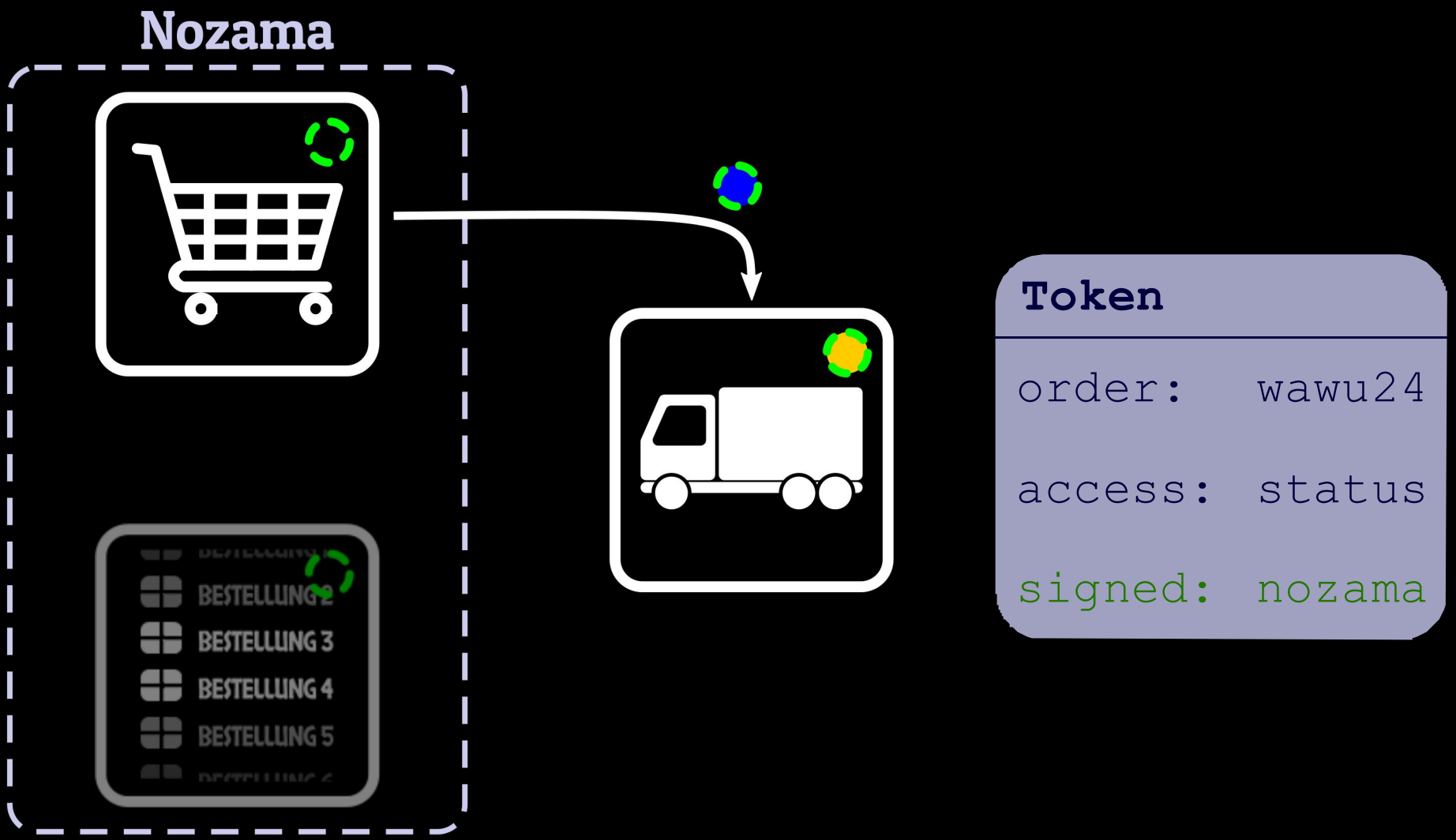
One-time password



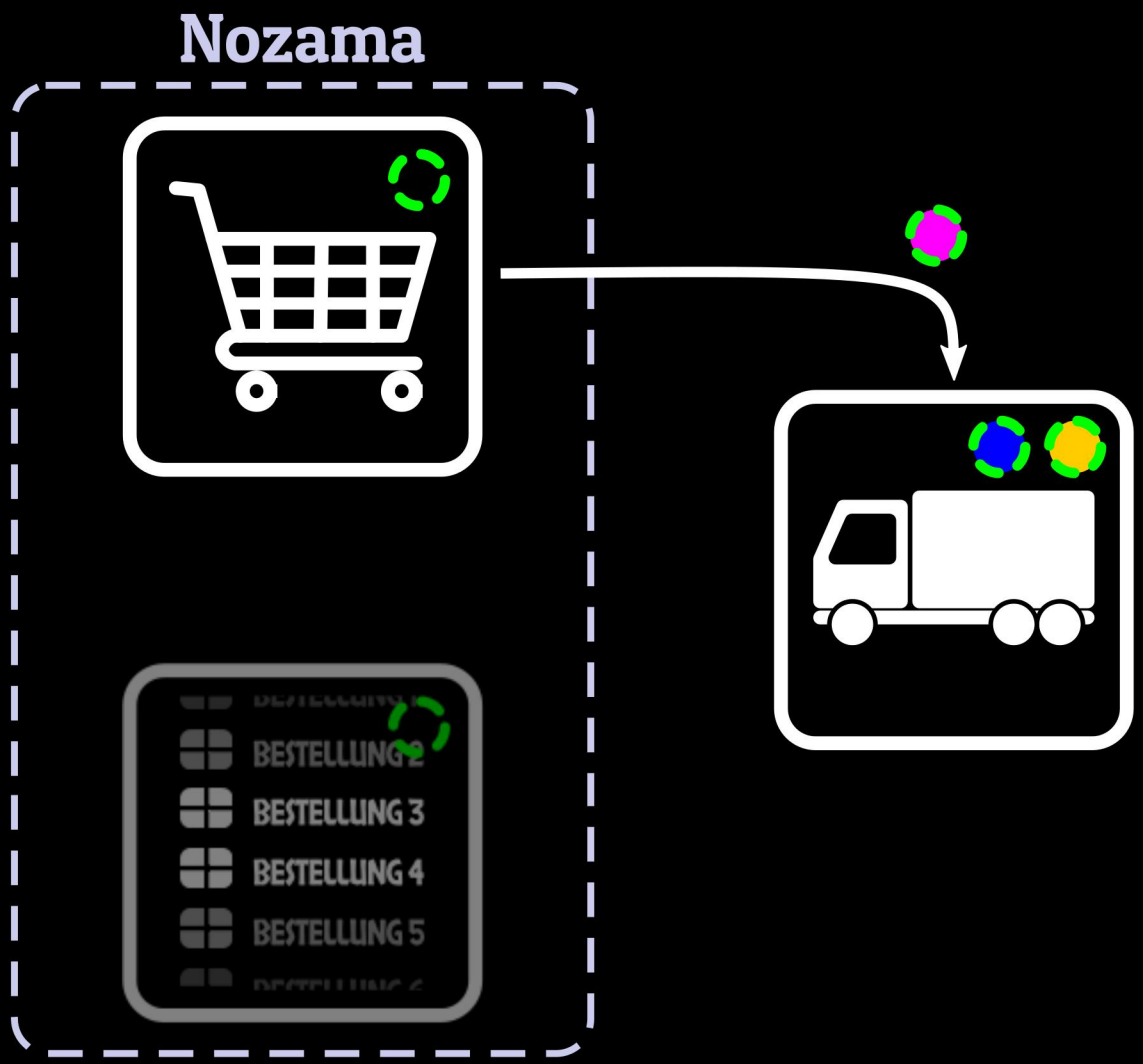
Token

```
order:   wawu23
access:  status
signed:  nozama
```

One-time password



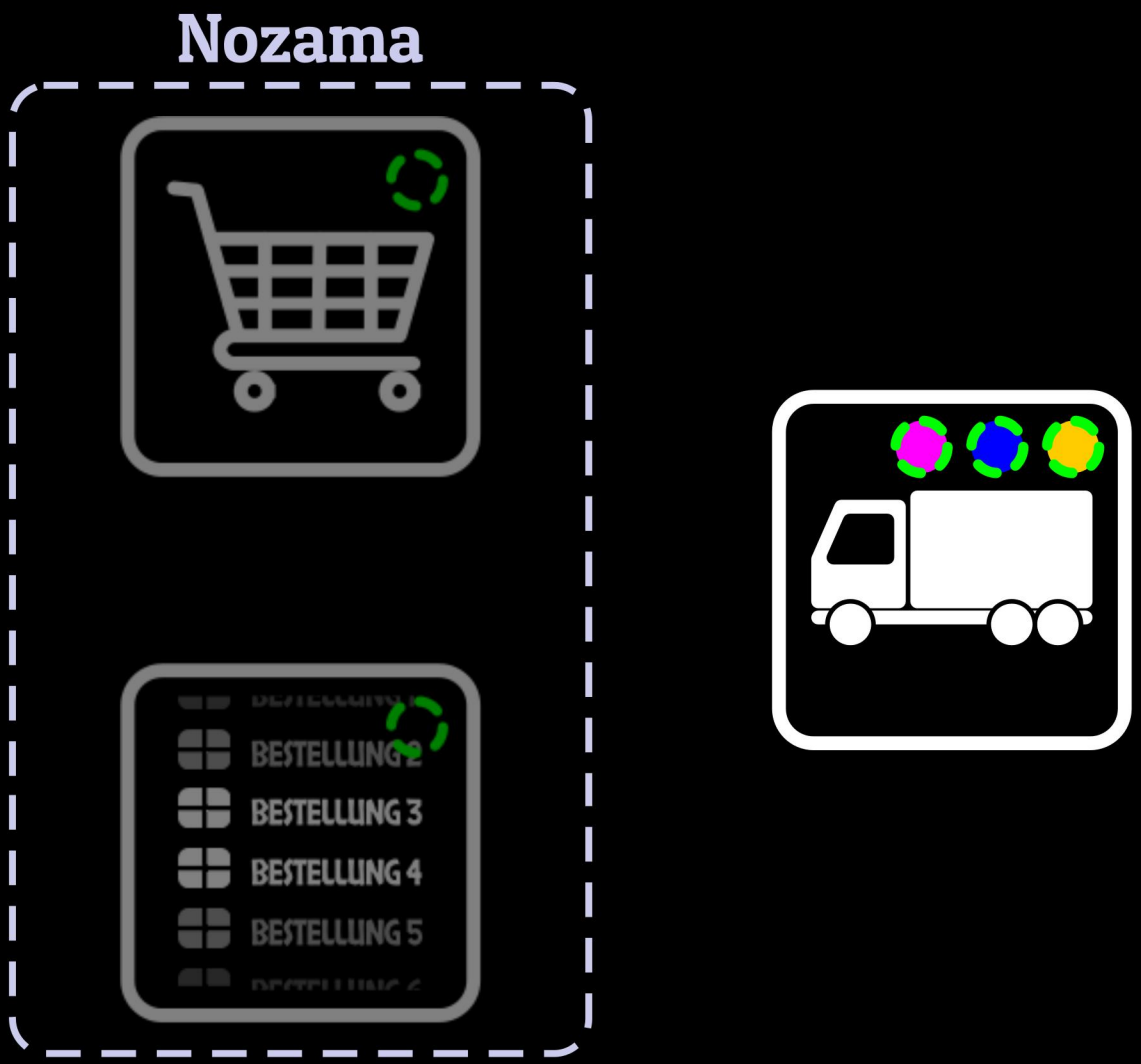
One-time password



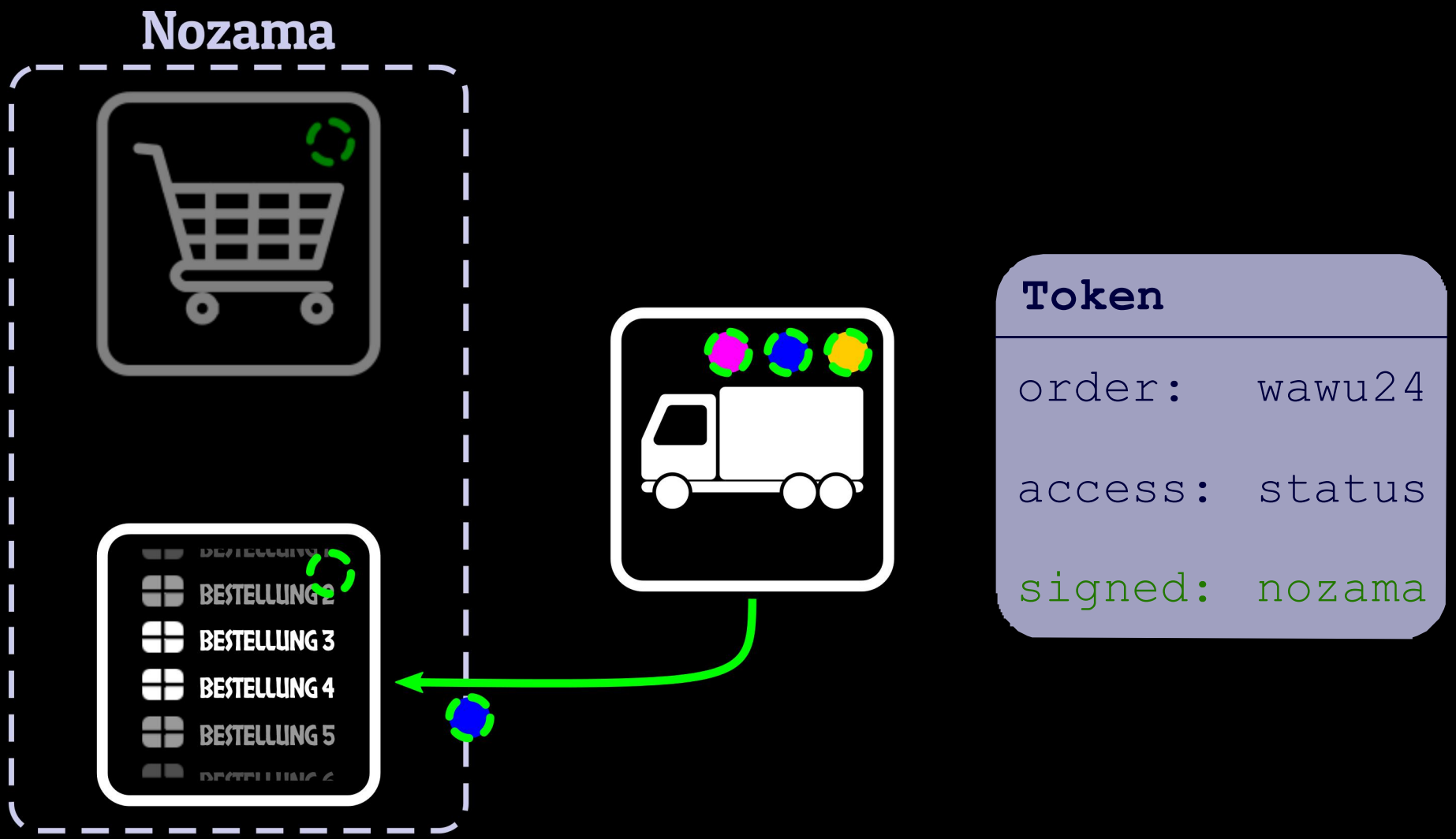
Token

```
order:   wawu25
access:  status
signed:  nozama
```

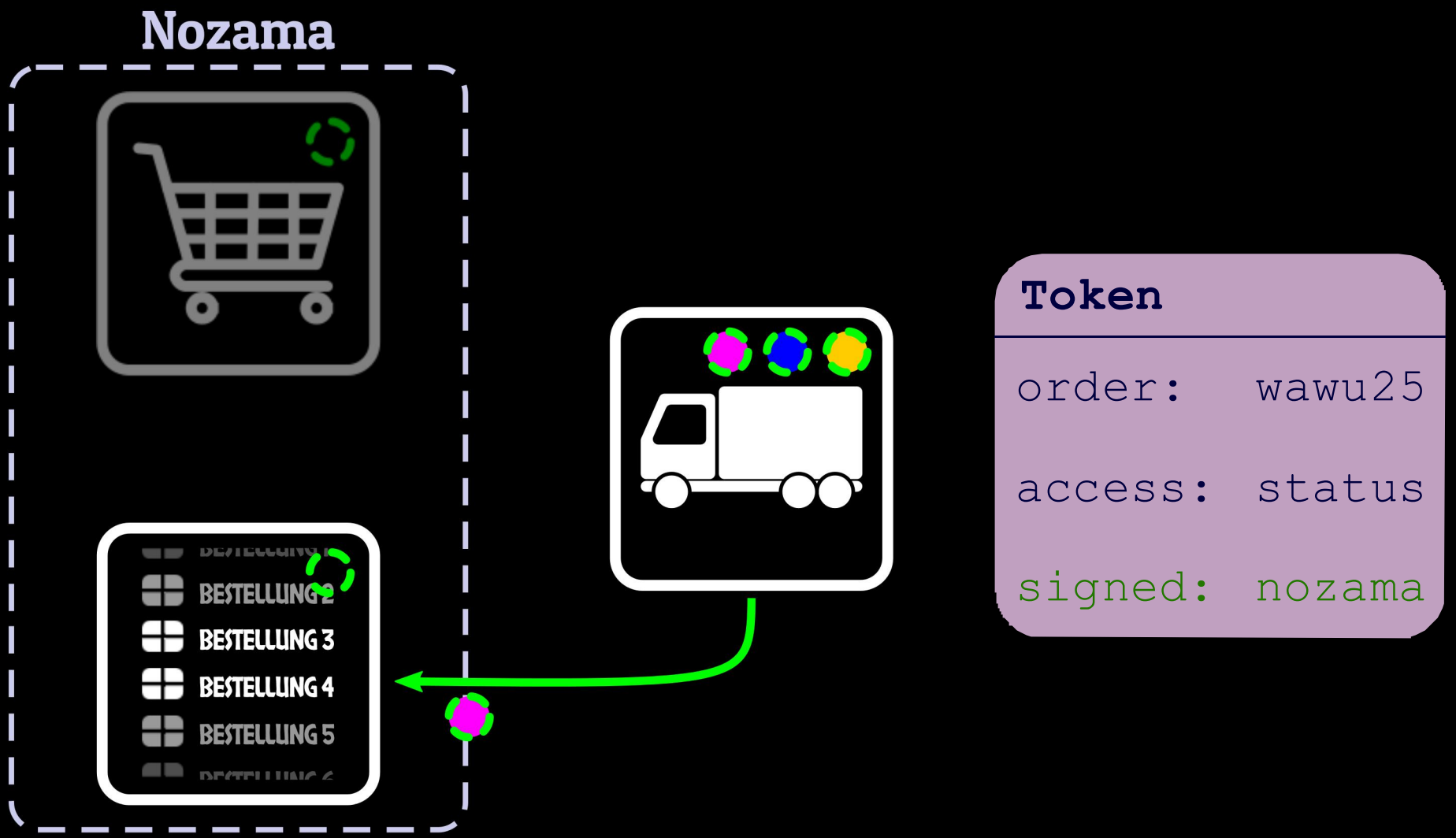
One-time password



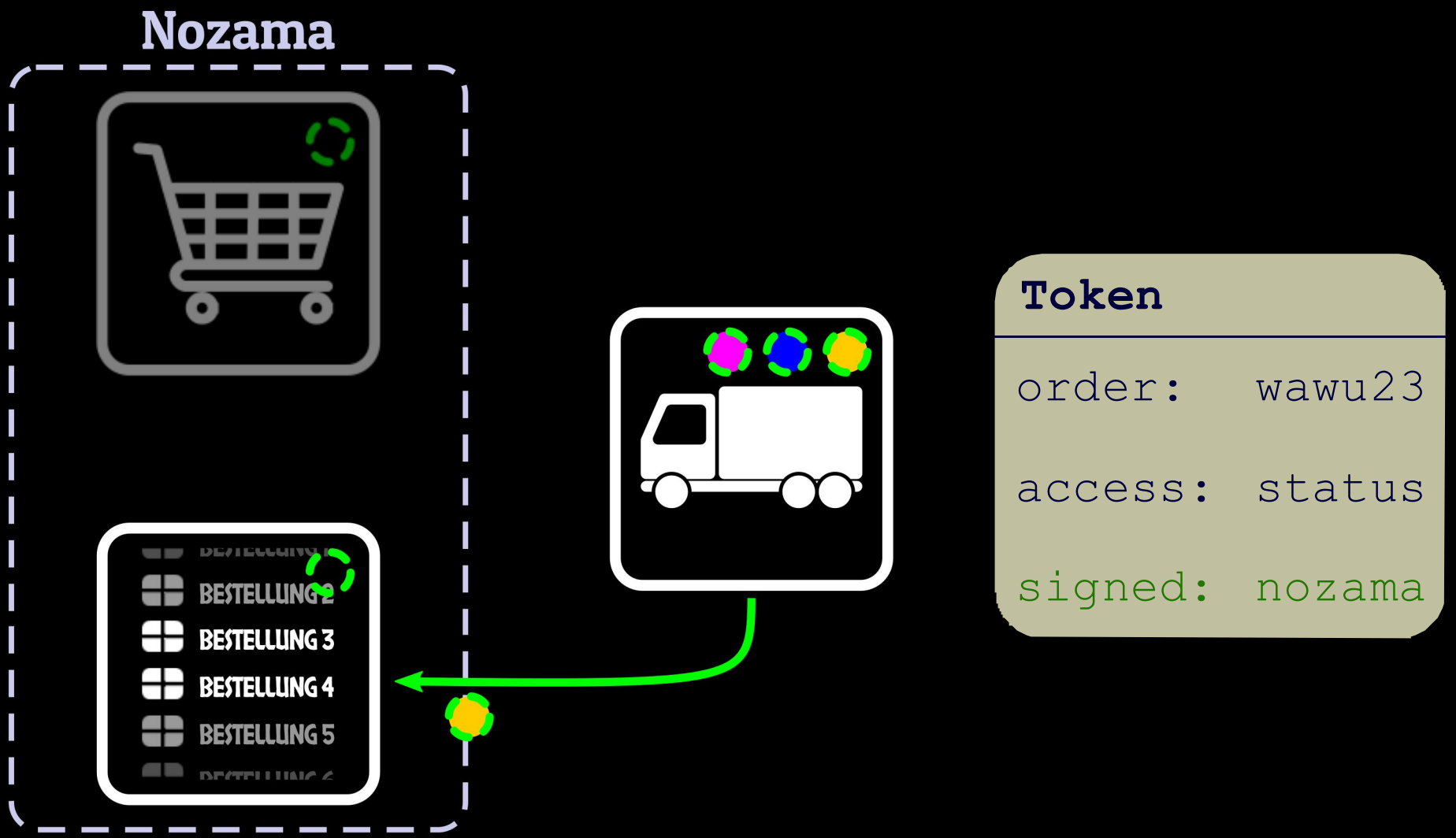
One-time password



One-time password

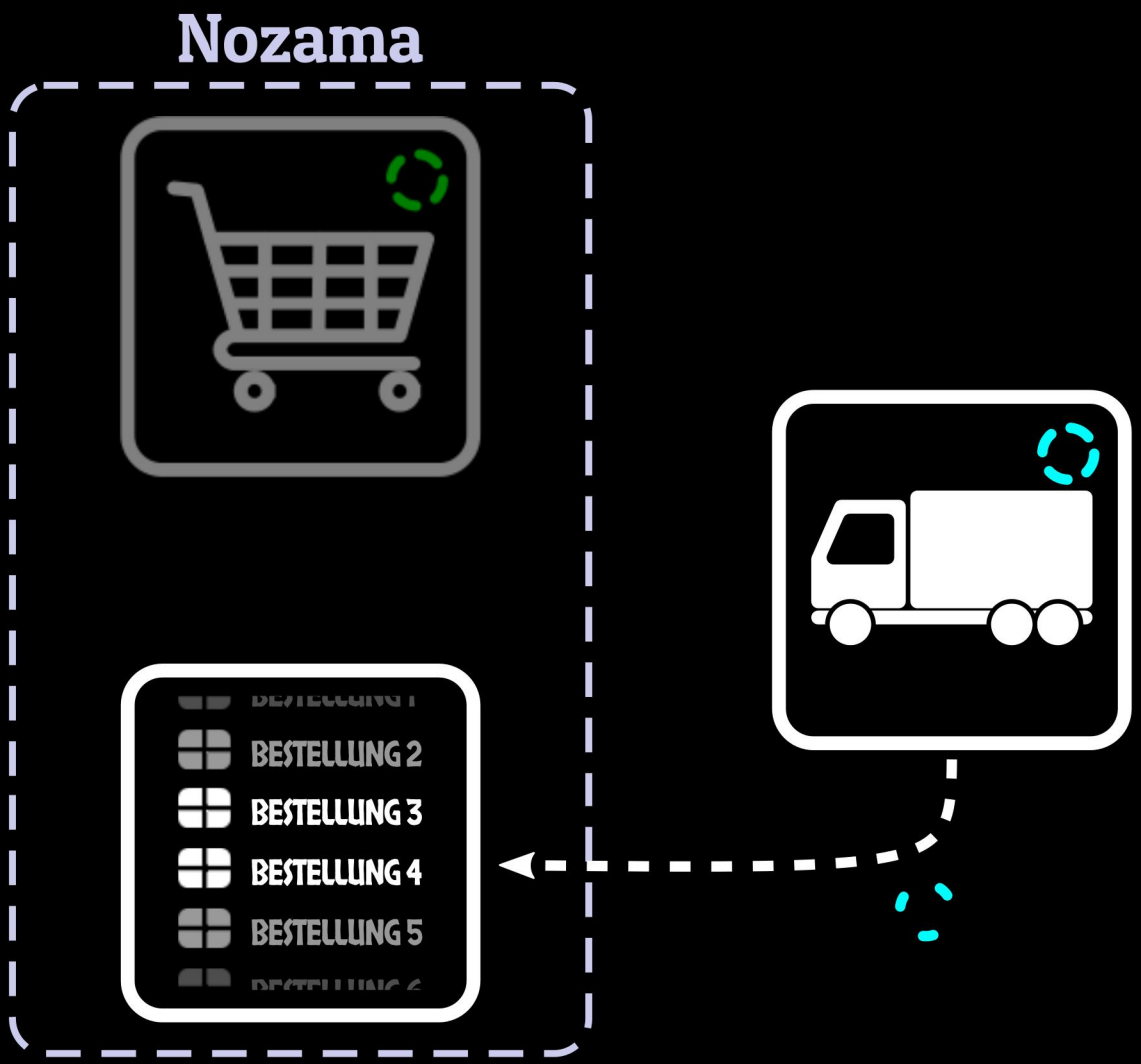


One-time password

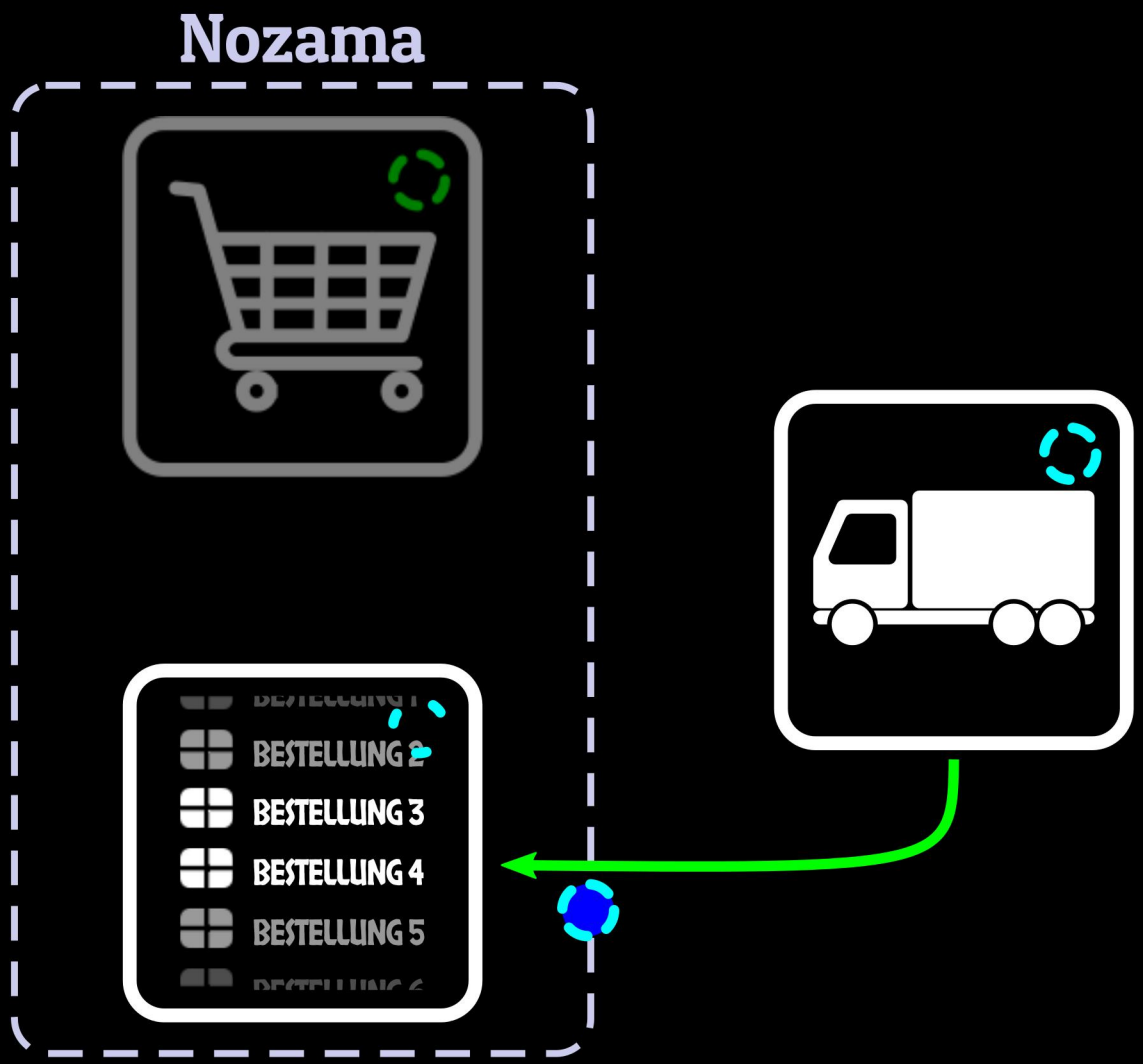


Peer to peer

Peer to peer

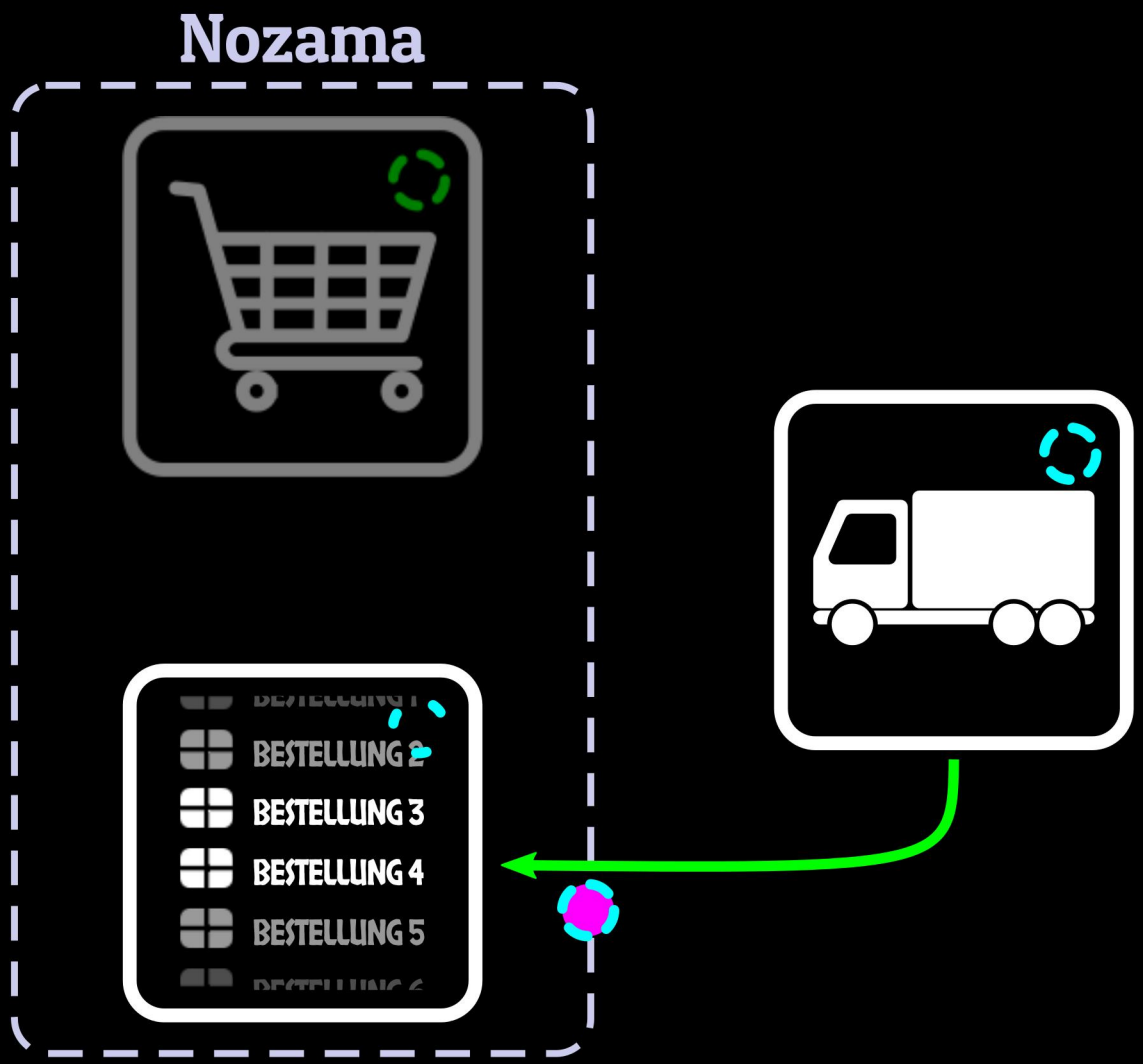

Nozama
BESTELLING 2
BESTELLING 3
BESTELLING 4
BESTELLING 5

Peer to peer



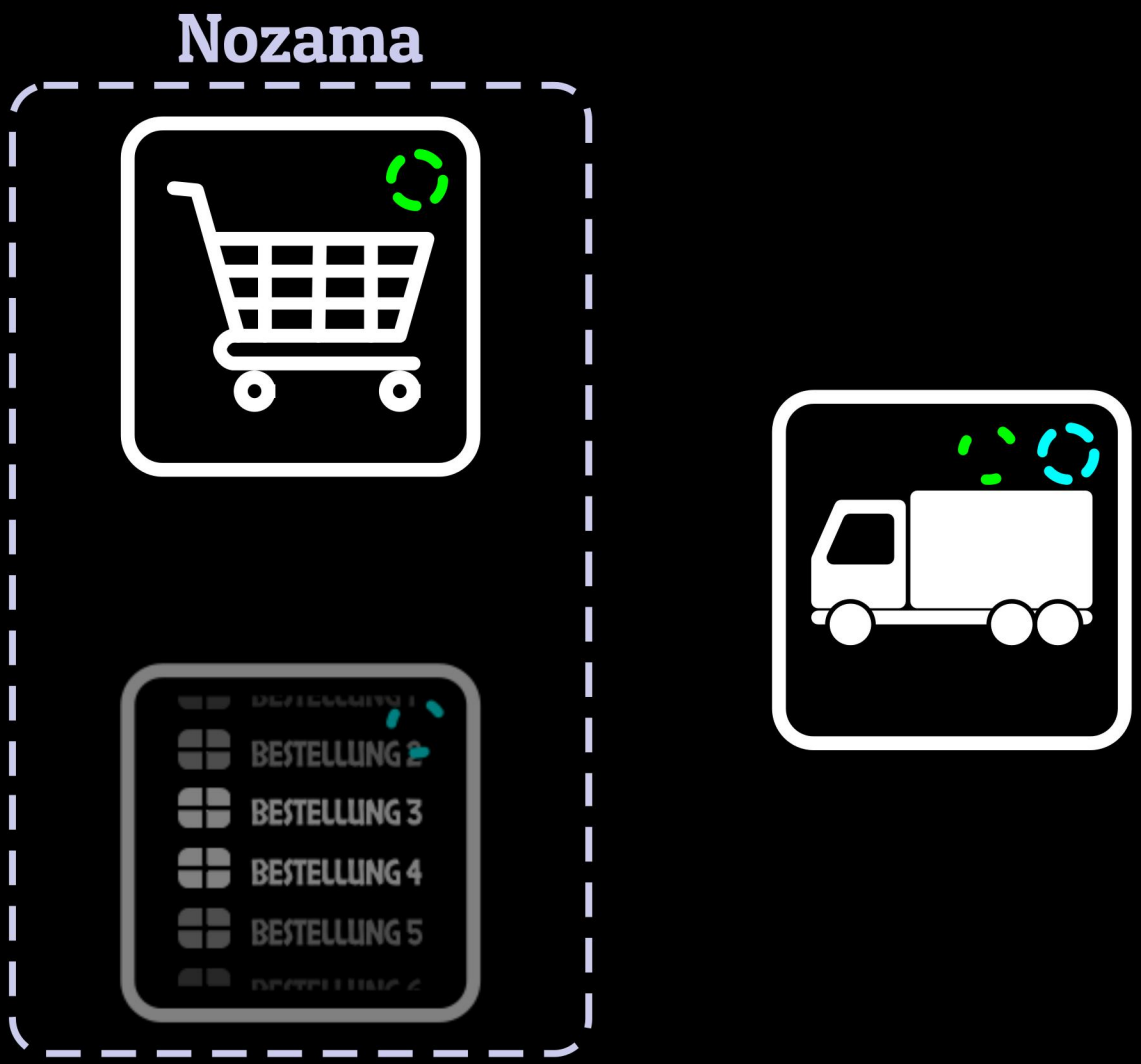

Token
id: trade64
challenge res1du3
expires: now+60s
signed: trader

Peer to peer

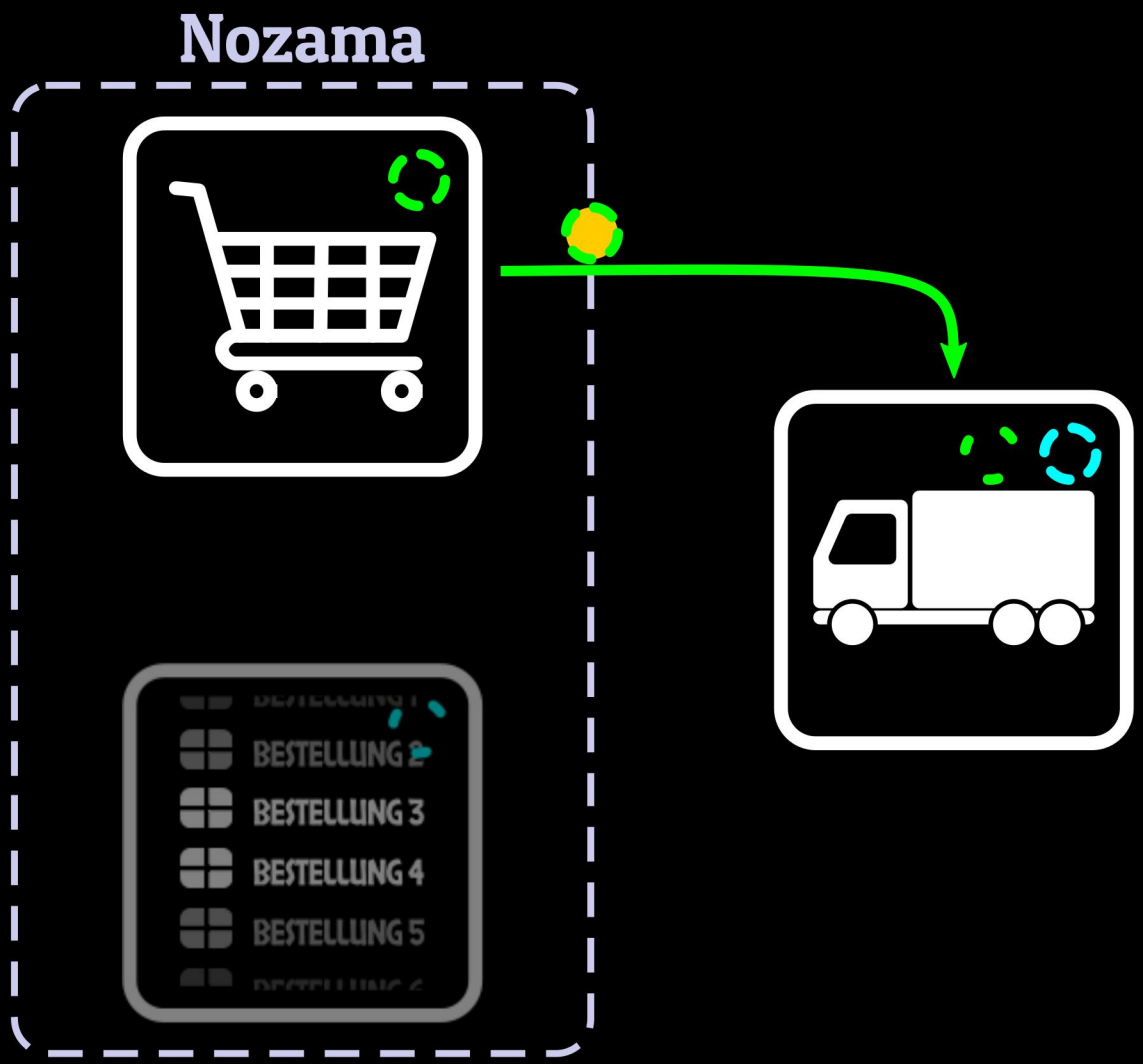


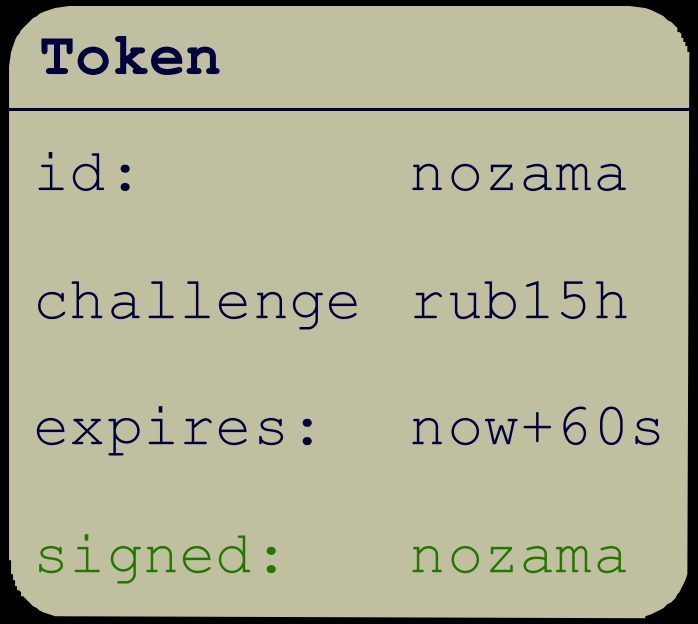

Token
id: trade64
challenge scr4p5
expires: now+60s
signed: trader

Peer to peer


Nozama
BESTELLING 2
BESTELLING 3
BESTELLING 4
BESTELLING 5

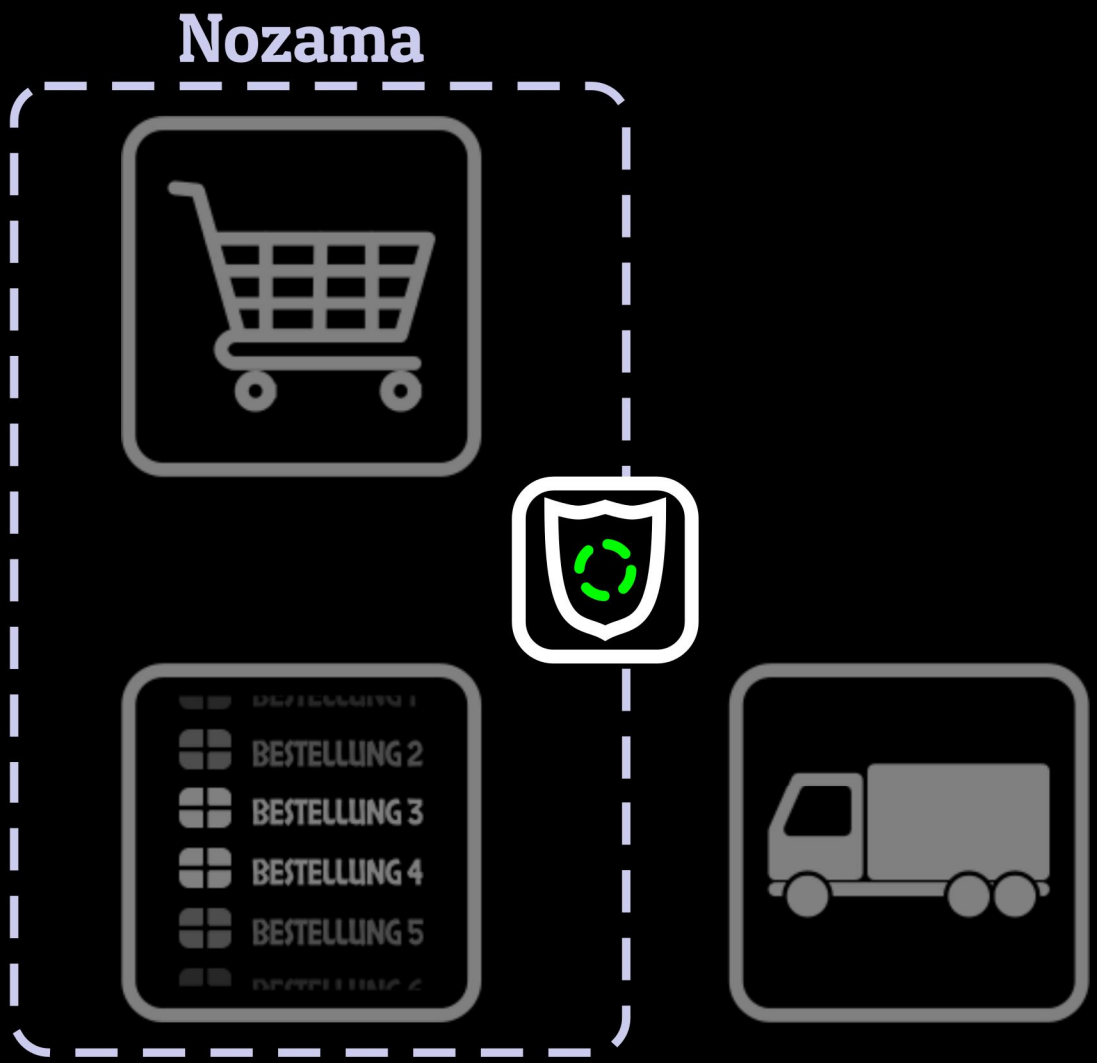
Peer to peer



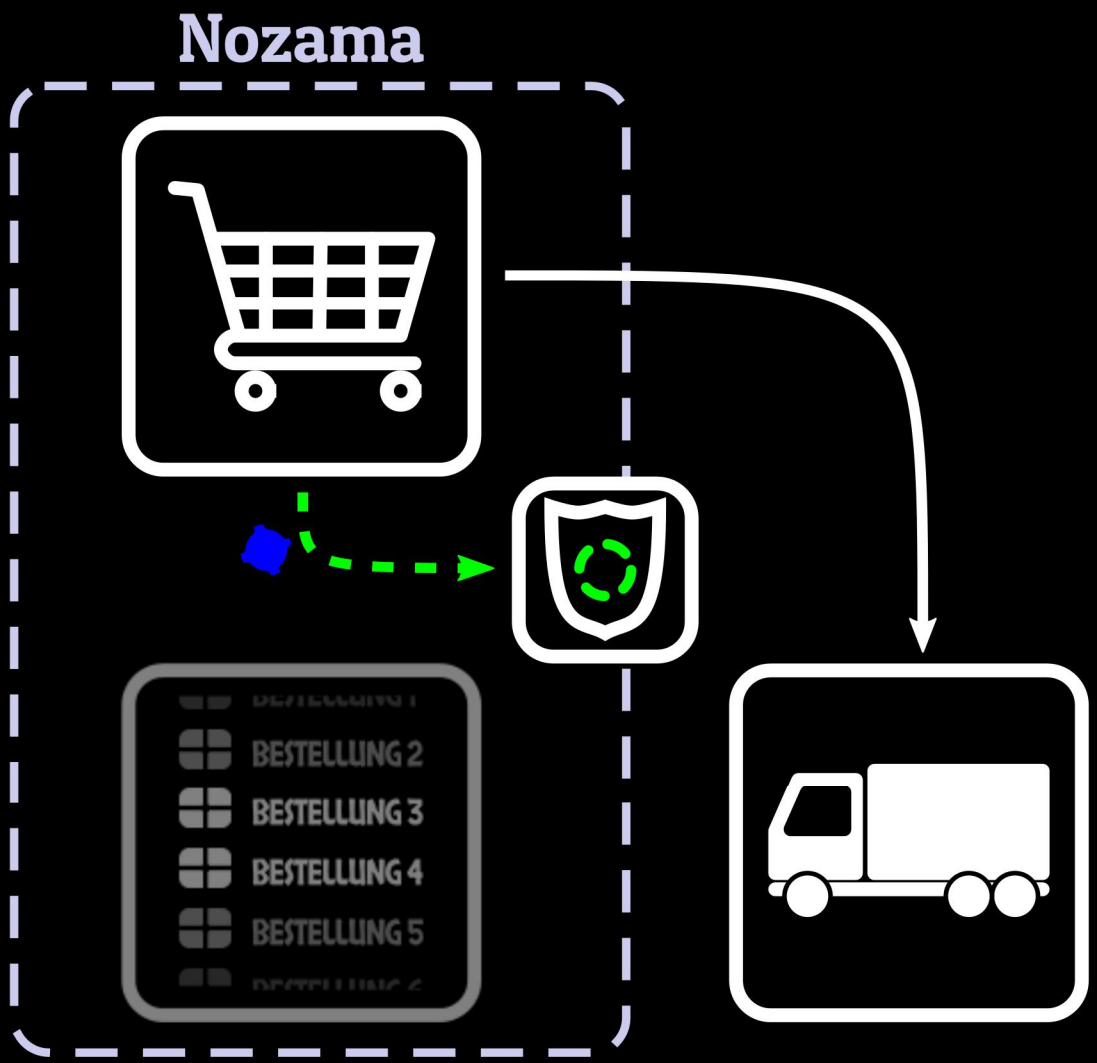

Token
id: nozama
challenge rub15h
expires: now+60s
signed: nozama

zentral

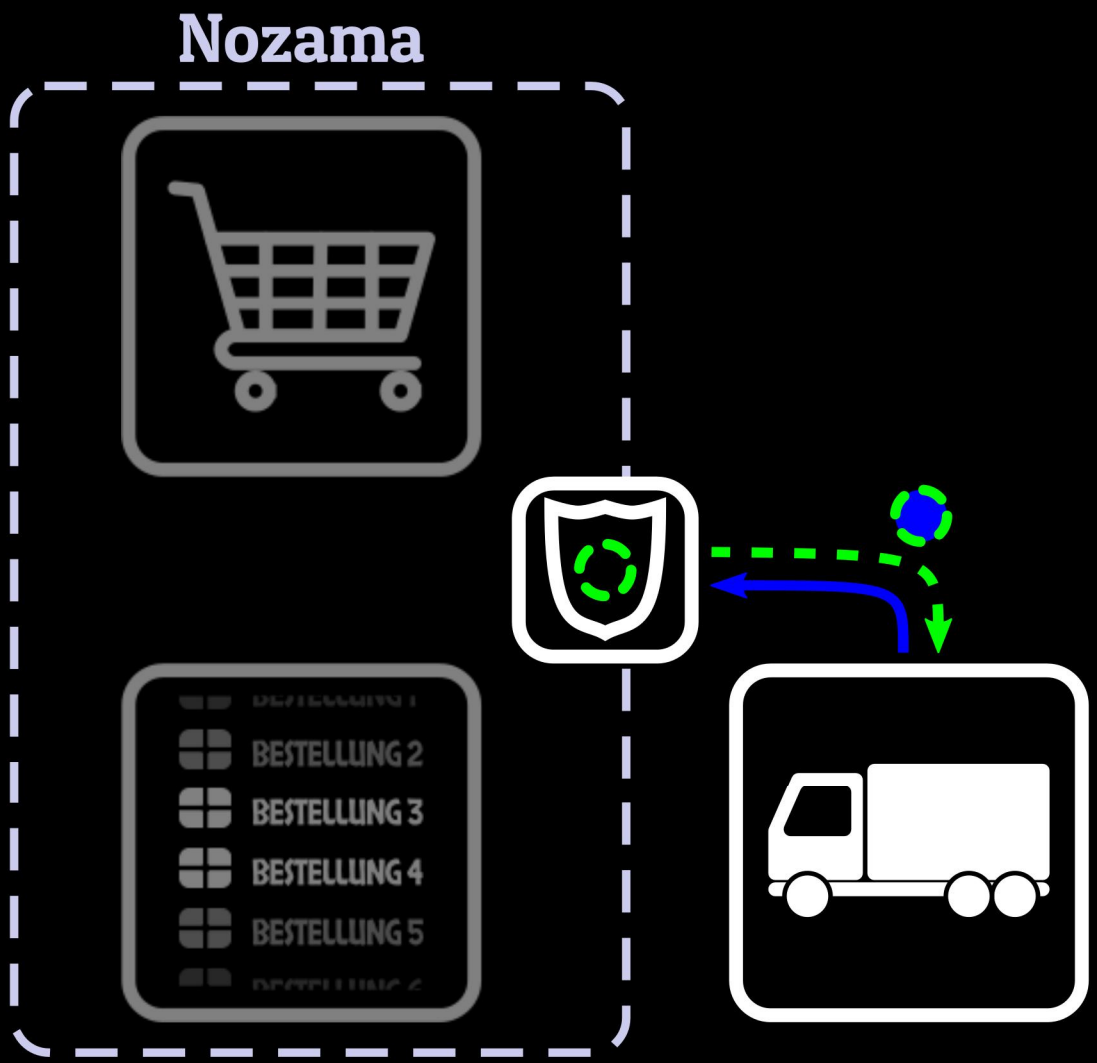
zentral


Nozama
BESTELLUNG 2
BESTELLUNG 3
BESTELLUNG 4
BESTELLUNG 5

zentral


Nozama
BESTELLUNG 2
BESTELLUNG 3
BESTELLUNG 4
BESTELLUNG 5

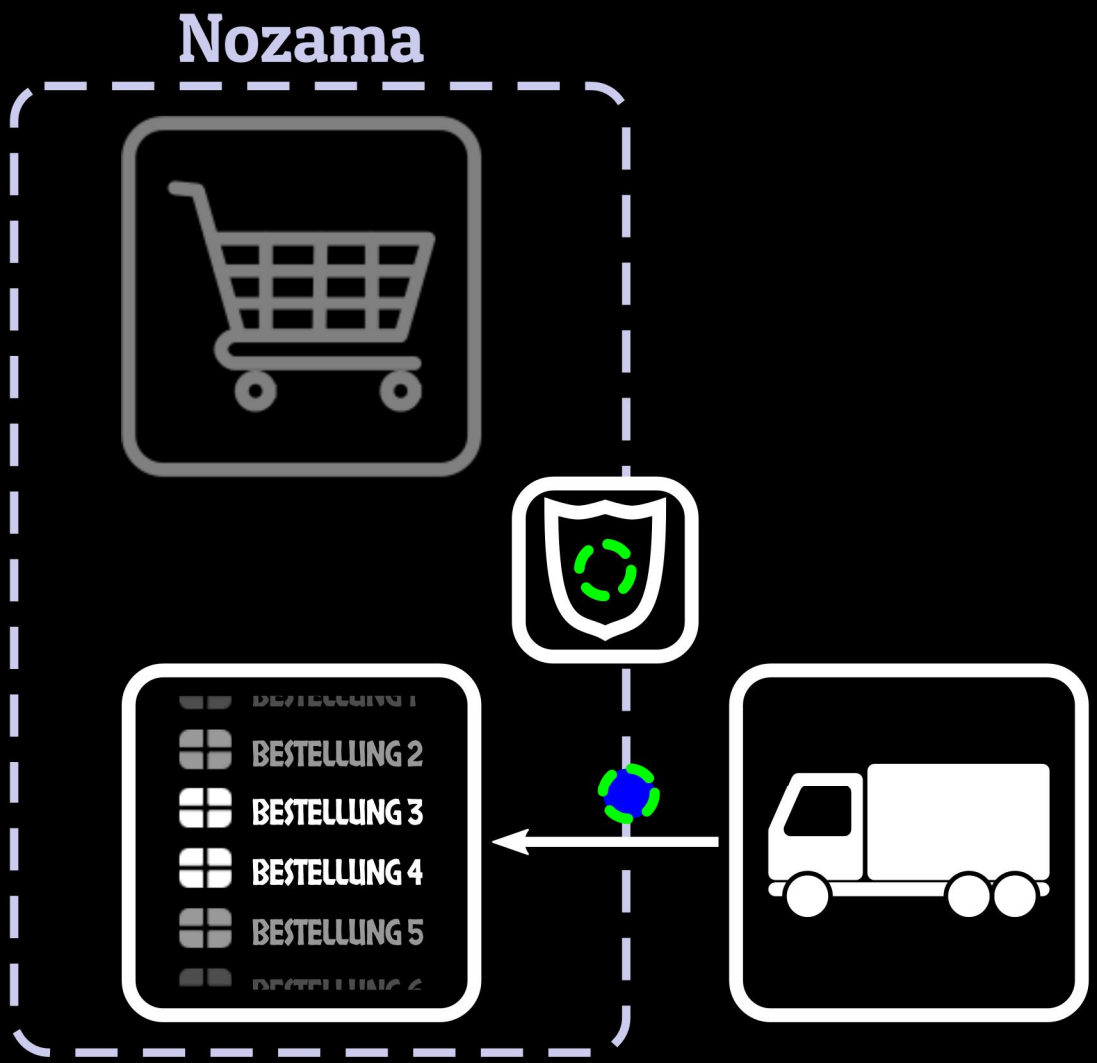
zentral



Token

order:	wawu23
access:	status
signed:	nozama

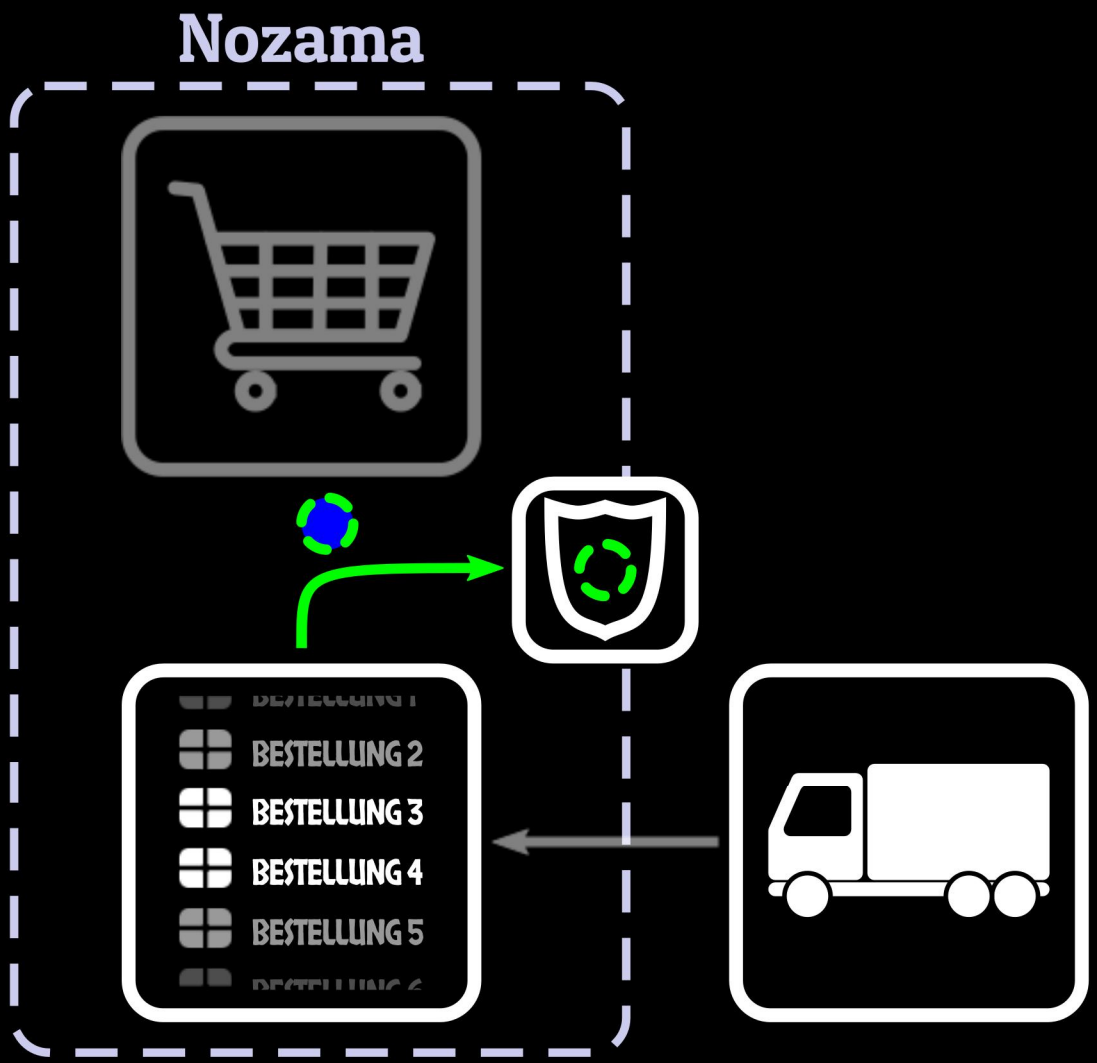
zentral



Token

order:	wawu23
access:	status
signed:	nozama

zentral

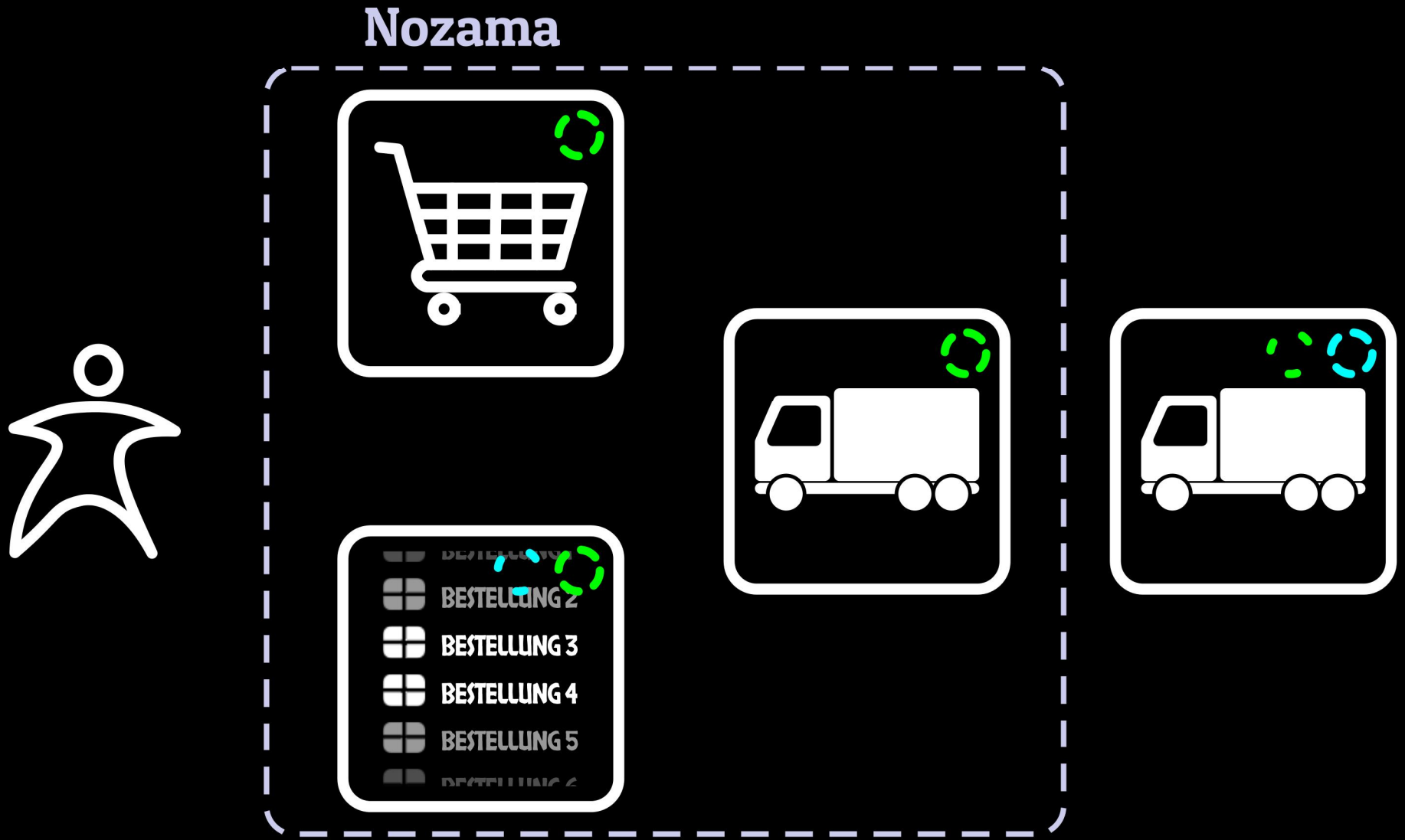


Token

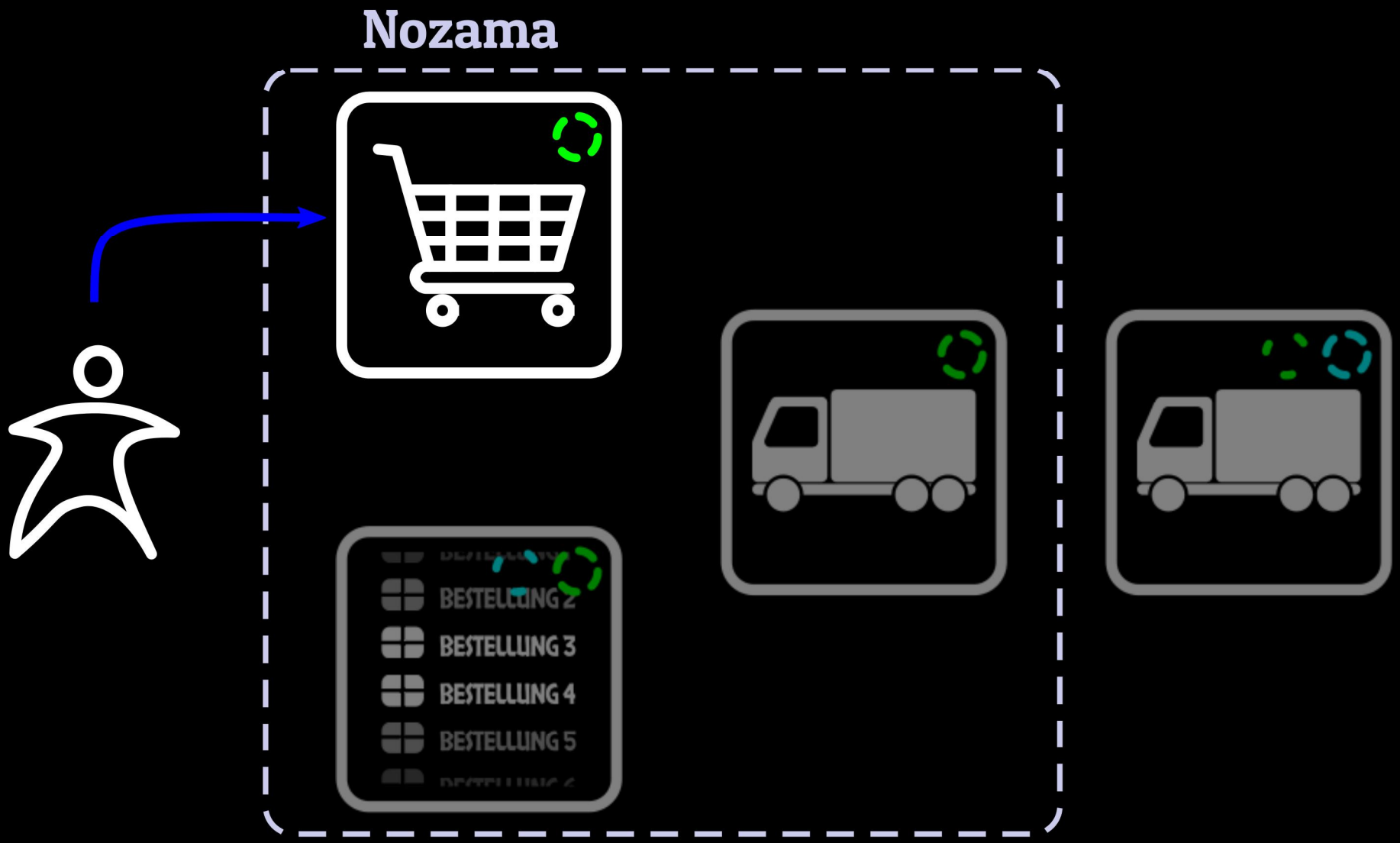
```
order:   wawu23
access:  status
signed:  nozama
```

Shopping

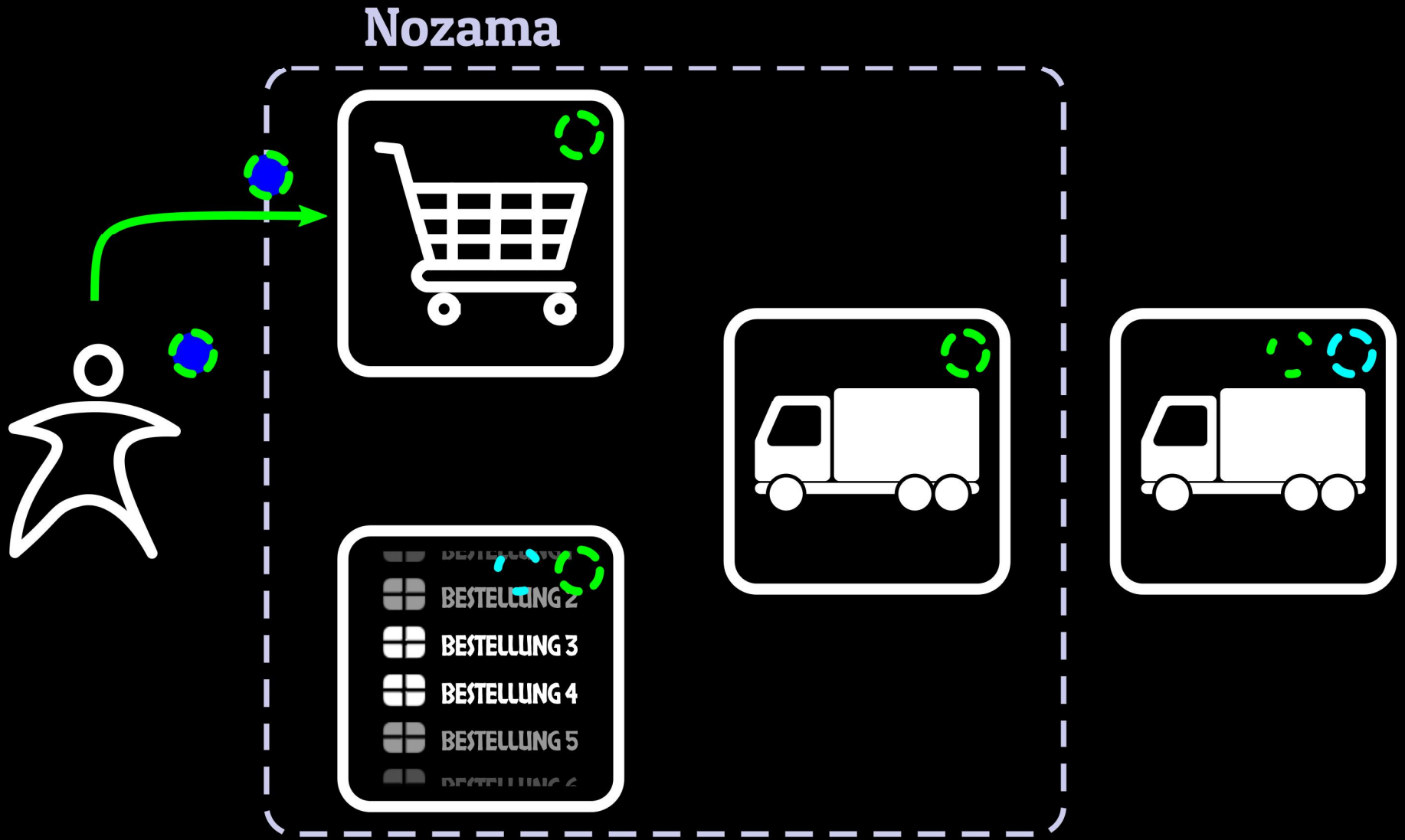
Shopping


Nozama
BESTELLUNG 2
BESTELLUNG 3
BESTELLUNG 4
BESTELLUNG 5

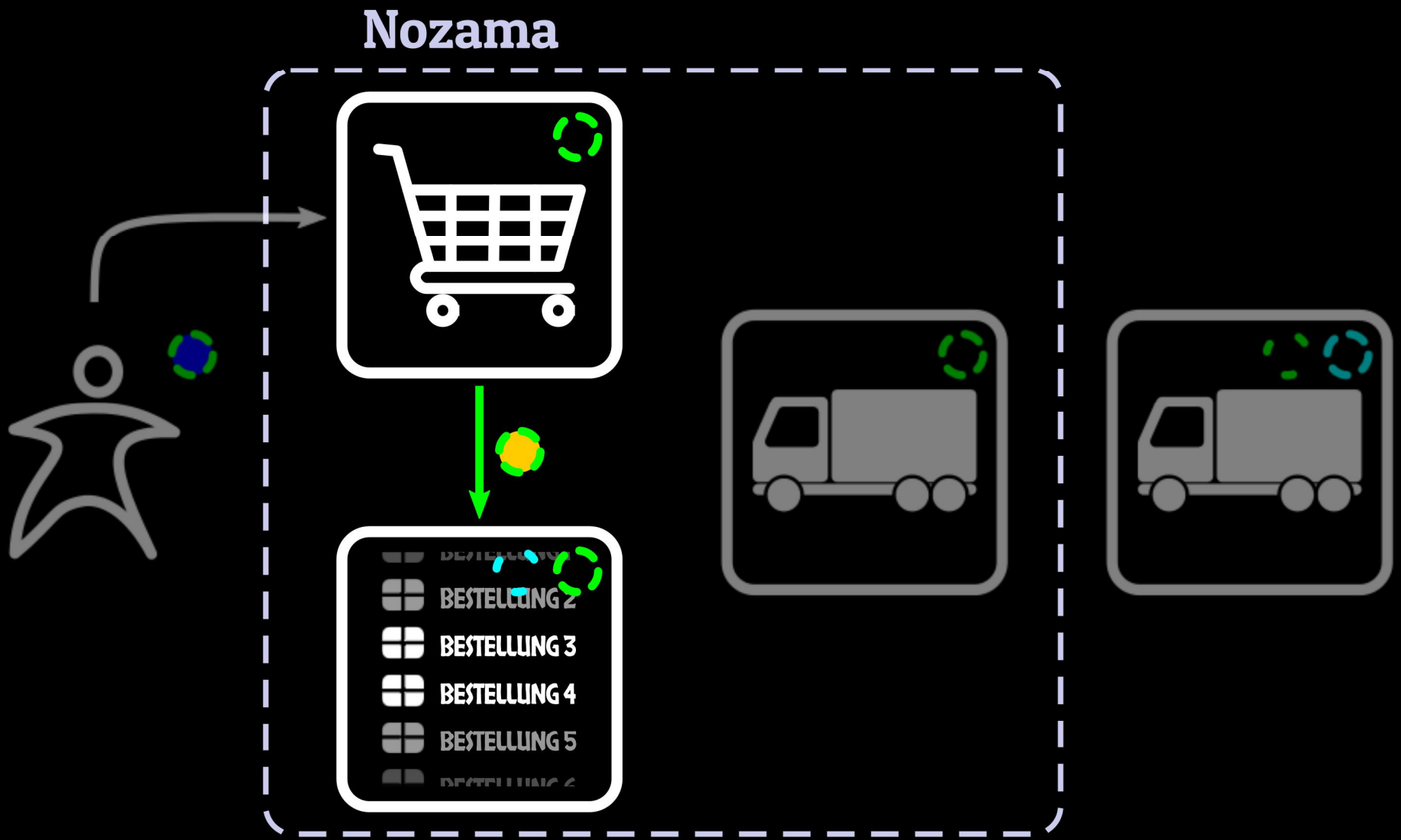
Shopping


Nozama
BESTELLING 2
BESTELLING 3
BESTELLING 4
BESTELLING 5

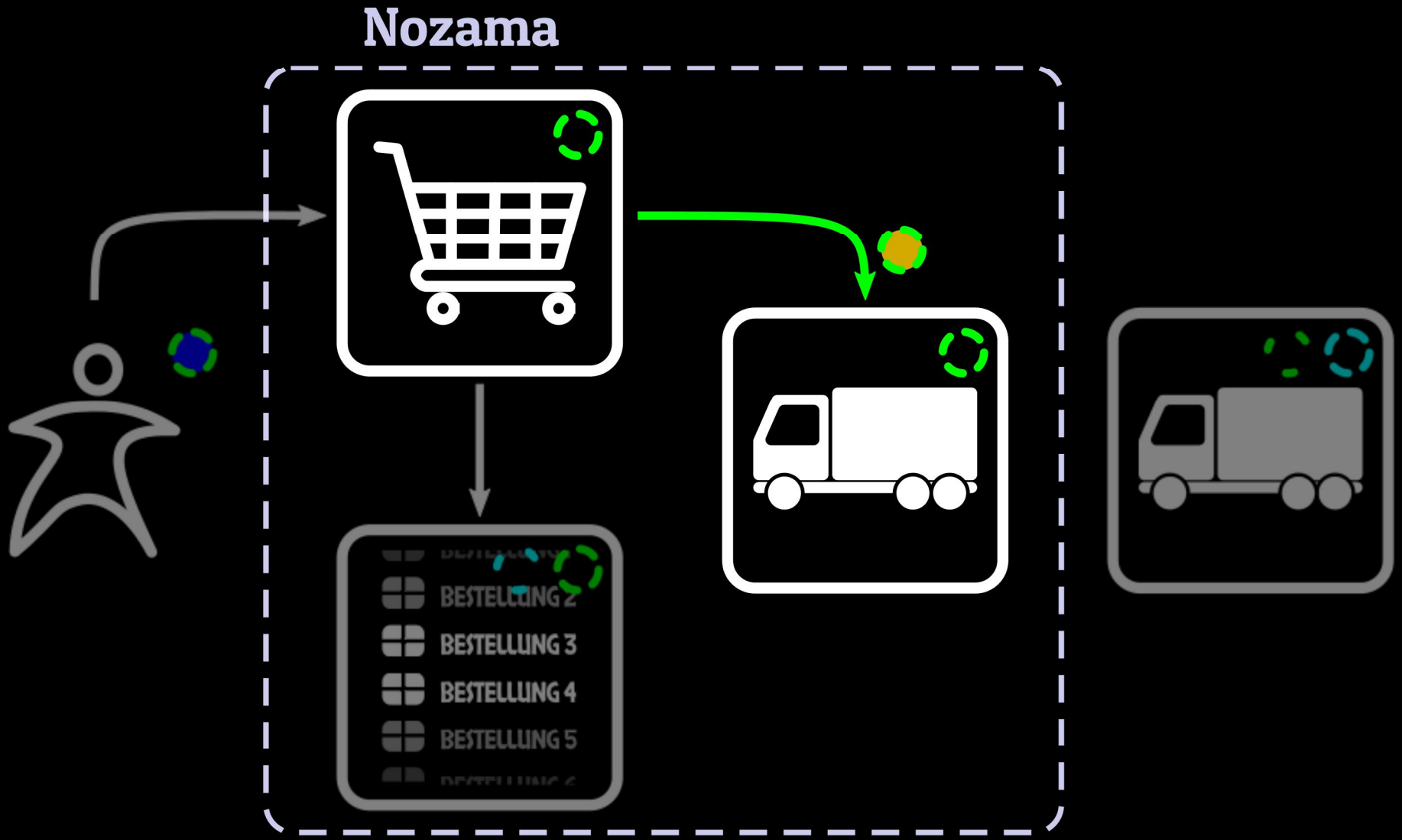
Shopping


Nozama
BESTELLUNG 2
BESTELLUNG 3
BESTELLUNG 4
BESTELLUNG 5

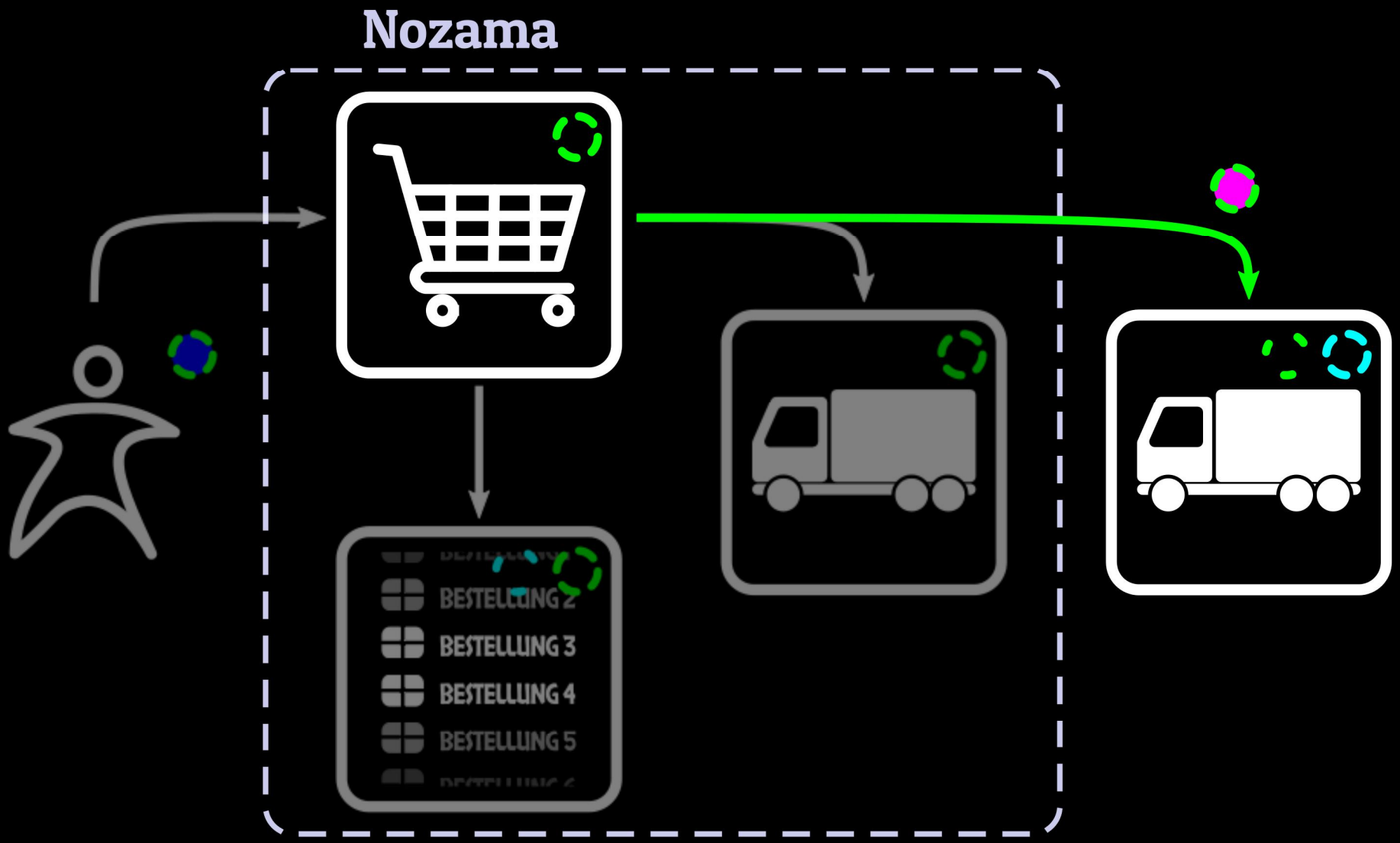
Shopping


Nozama
BESTELLUNG 2
BESTELLUNG 3
BESTELLUNG 4
BESTELLUNG 5

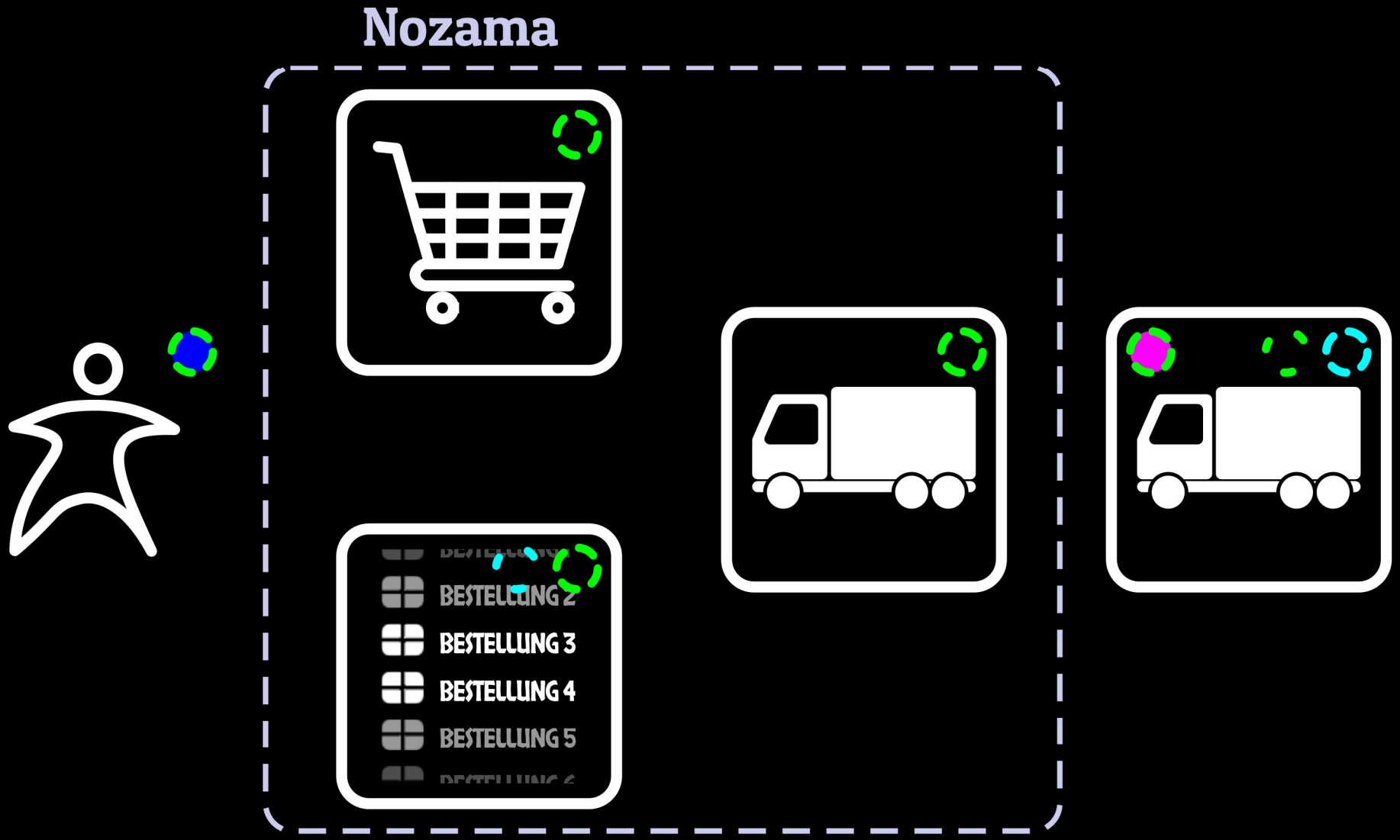
Shopping


Nozama
BESTELLING 2
BESTELLING 3
BESTELLING 4
BESTELLING 5

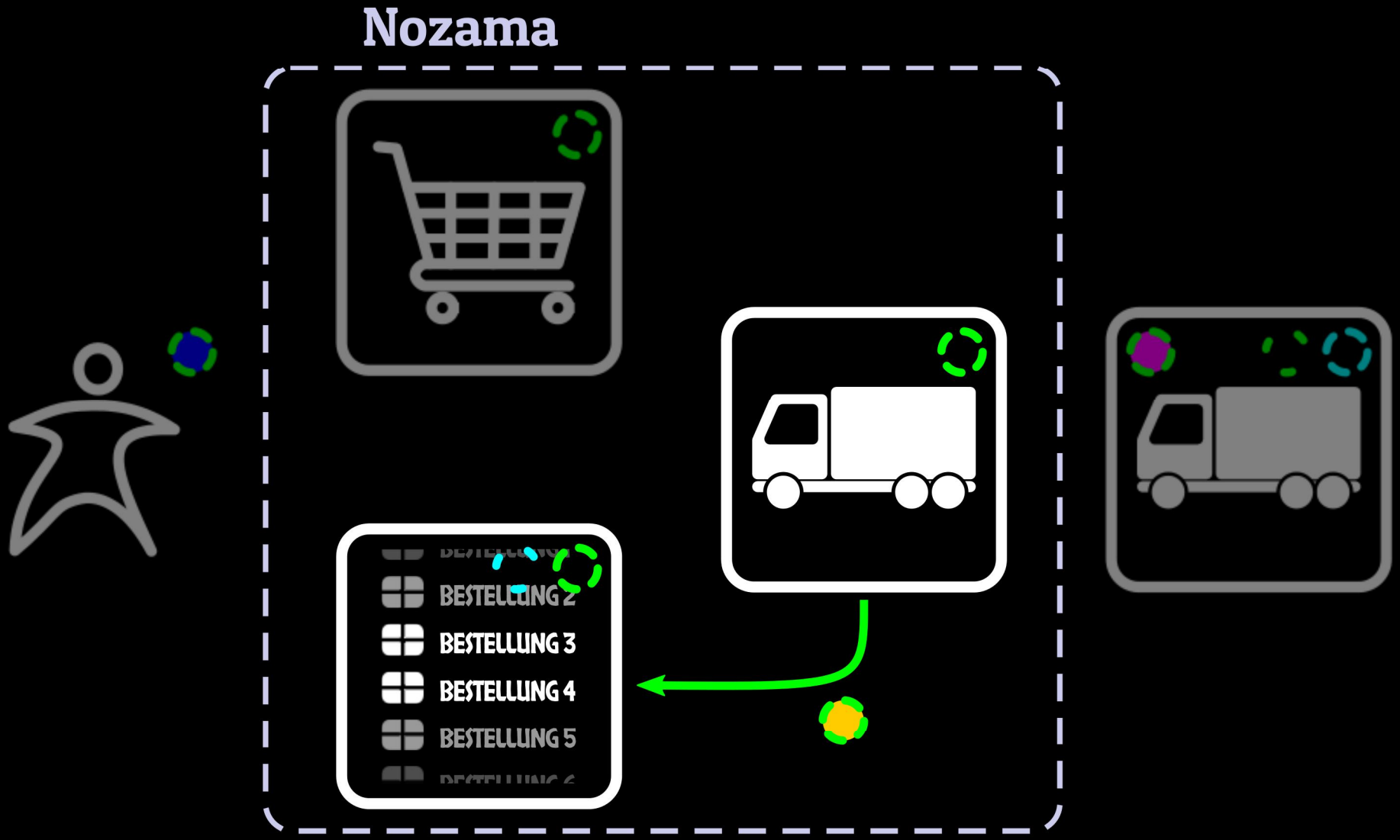
Shopping


Nozama
BESTELLING 2
BESTELLING 3
BESTELLING 4
BESTELLING 5

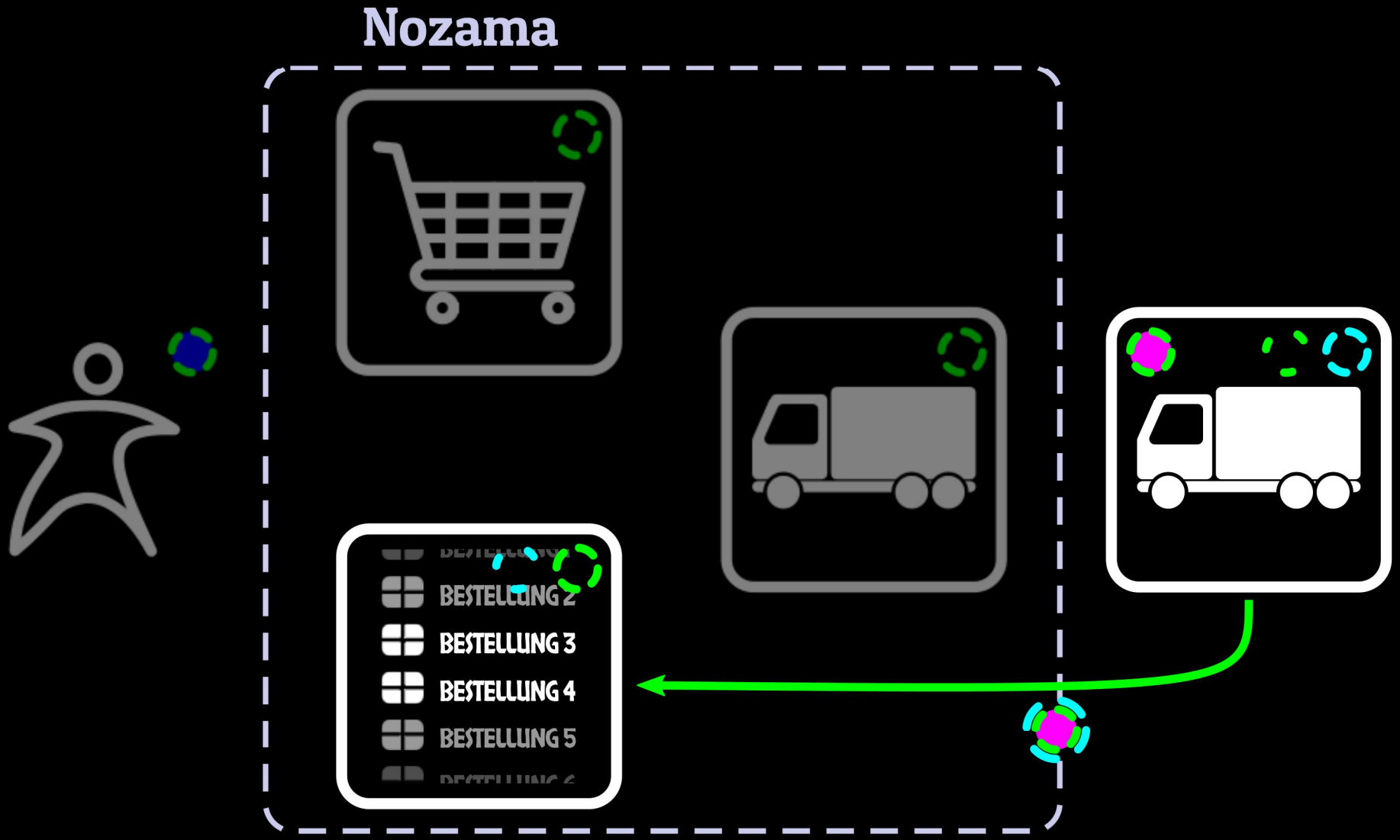
Shopping


Nozama
BESTELLUNG 2
BESTELLUNG 3
BESTELLUNG 4
BESTELLUNG 5

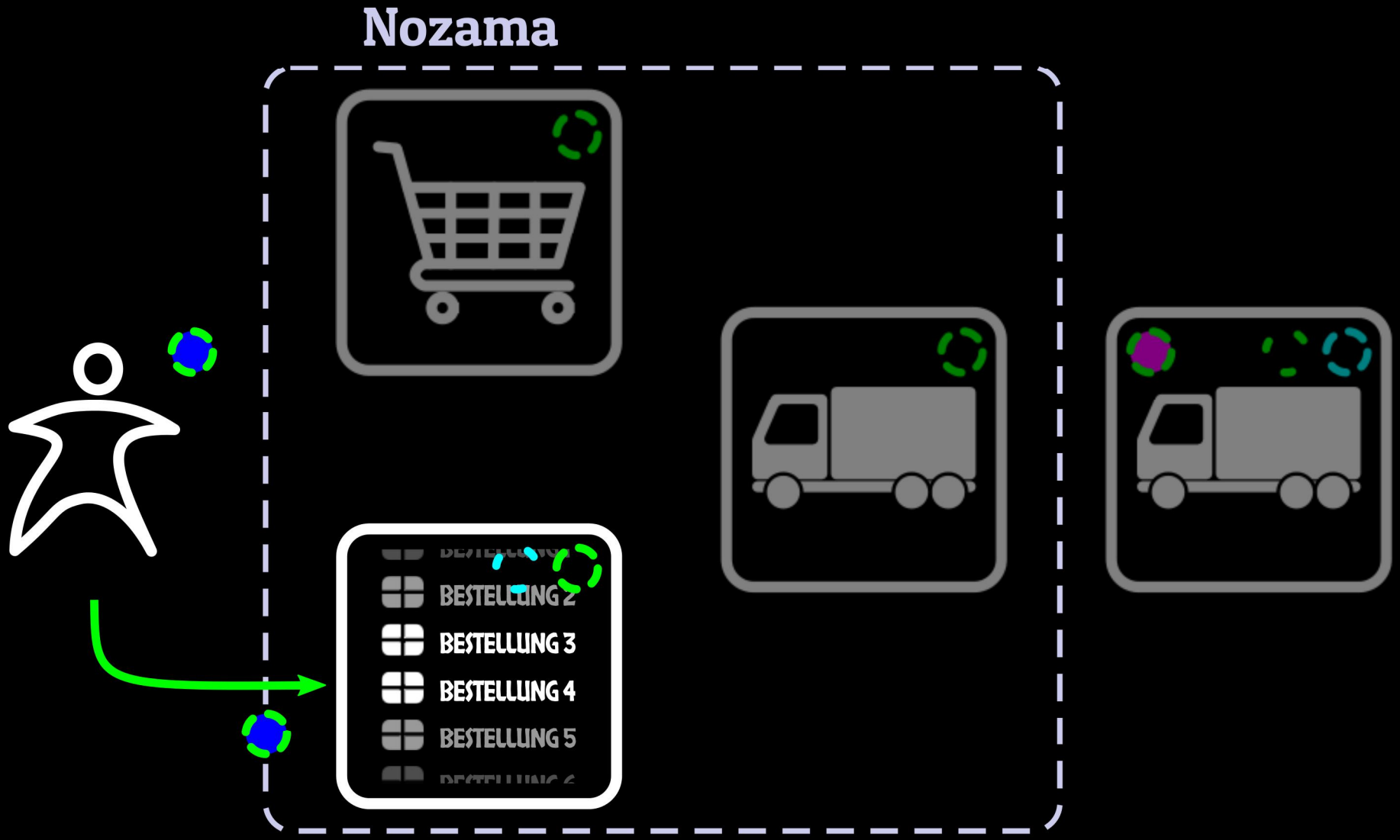
Shopping


Nozama
BESTELLUNG 2
BESTELLUNG 3
BESTELLUNG 4
BESTELLUNG 5

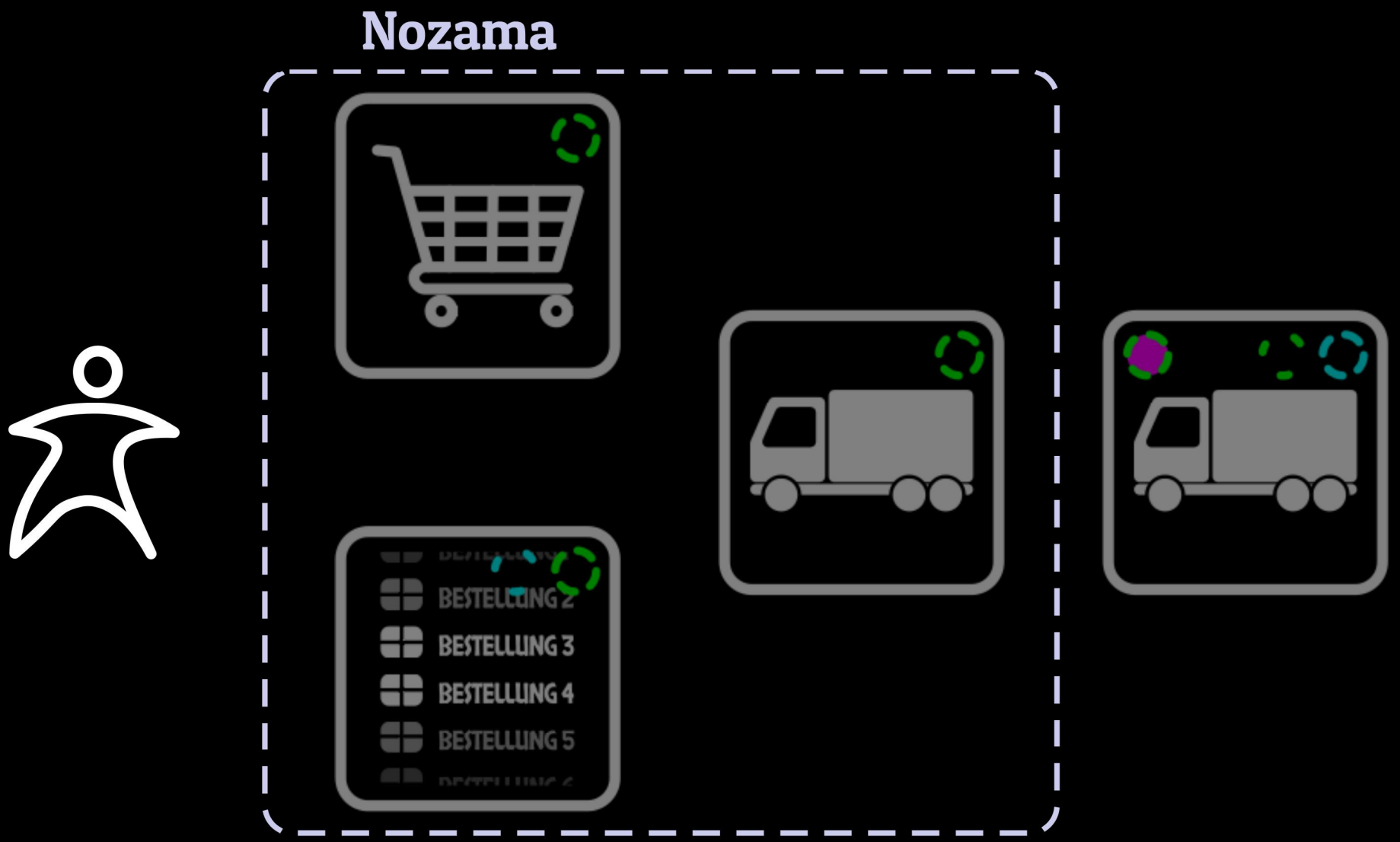
Shopping


Nozama
BESTELLUNG 2
BESTELLUNG 3
BESTELLUNG 4
BESTELLUNG 5

Shopping


Nozama
BESTELLUNG 2
BESTELLUNG 3
BESTELLUNG 4
BESTELLUNG 5

Shopping


Nozama
BESTELLING 2
BESTELLING 3
BESTELLING 4
BESTELLING 5

Fazit

- Zugriffskontrolle integralen Bestandteil Microservicearchitektur.
- Microservice-Landschaft -> wichtiger -> Zugriffskontrolle -> gezielt und flexibel
- Tokens für unterschiedliche Zugriffsmodelle
- Mittel um Flexibilitaet zu ermöglichen.
- Erfahrungen: Akzeptanz durch Entwickler, interner & externer Systeme