

MAINFRAME MEERWAARDE - PVIB.NL

Run presentation from the start
Start in kiosk-mode

Automatic start in 3 seconds...

MAINFRAME MEERWAARDE - PVIB.NL

Run presentation from the start
Start in kiosk-mode

Automatic start in 3 seconds...

MAINFRAME MEERWAARDE - PVIB.NL

Run presentation from the start
Start in kiosk-mode

Automatic start in 2 seconds...

MAINFRAME MEERWAARDE - PVIB.NL

Run presentation from the start
Start in kiosk-mode

Automatic start in 2 seconds...

MAINFRAME MEERWAARDE - PVIB.NL

Run presentation from the start
Start in kiosk-mode

Automatic start in 1 seconds...

MAINFRAME MEERWAARDE - PVIB.NL

Run presentation from the start
Start in kiosk-mode

Automatic start in 0 seconds...

[] Starting Switch Presenter...

```
[ ] Starting Switch Presenter...  
[ OK ] Started rebuild Dynamic Audience Participation Amplifier.
```

```
[ ] Starting Switch Presenter...  
[ OK ] Started rebuild Dynamic Audience Participation Amplifier.  
[ ] Starting Update is Completed...
```

```
[ ] Starting Switch Presenter...
[ OK ] Started rebuild Dynamic Audience Participation Amplifier.
[ ] Starting Update is Completed...
[ OK ] Started Update is Completed.
[ OK ] Reached target System Initialization.
```

```
[ ] Starting Switch Presenter...
[ OK ] Started rebuild Dynamic Audience Participation Amplifier.
[ ] Starting Update is Completed...
[ OK ] Started Update is Completed.
[ OK ] Reached target System Initialization.
[ OK ] Starting Update is Completed.
[ OK ] Listening on standard Q&A socket.
[ OK ] Starting Update is Completed.
[ OK ] Reached ready mode.
```

[DISCLAIMER - LEGAL NOTICE]

The thoughts, ideas, and digital musings shared in this session are provided on an “as-is” basis, with no warranty, expressed or implied. They are intended solely for educational purposes and may or may not have been approved by my employer, or any other authority figures (real or imagined).

Users are hereby nerdy-nudged to refrain from applying any of the knowledge or techniques discussed herein without prior, explicit authorization from their respective system administrators, IT overlords, or other appropriate authority figures.

Unauthorized use may result in a stern talking-to, a temporary ban from the coffee machine, or worse—being assigned to a meeting with no coffee.

[[CONTINUE](#)] [CANCEL]


```
[ ] Starting Switch Presenter...
[ OK ] Started rebuild Dynamic Audience Participation Amplifier.
[ ] Starting Update is Completed...
[ OK ] Started Update is Completed.
[ OK ] Reached target System Initialization.
[ OK ] Starting Update is Completed.
[ OK ] Listening on standard Q&A socket.
[ OK ] Starting Update is Completed.
[ OK ] Reached ready mode.
[ OK ] Starting Update is Completed.
[ ] Starting Audio Module...
```

```
[ Starting Switch Presenter...
[ OK Started rebuild Dynamic Audience Participation Amplifier.
[ Starting Update is Completed...
[ OK Started Update is Completed.
[ OK Reached target System Initialization.
[ OK Starting Update is Completed.
[ OK Listening on standard Q&A socket.
[ OK Starting Update is Completed.
[ OK Reached ready mode.
[ OK Starting Update is Completed.
Starting Audio Module...
Starting Service enabling compressing RAM with zRam...
Starting Hold until boot process finishes up...
```

```
[ ] Starting Switch Presenter...
[ OK ] Started rebuild Dynamic Audience Participation Amplifier.
[ ] Starting Update is Completed...
[ OK ] Started Update is Completed.
[ OK ] Reached target System Initialization.
[ OK ] Starting Update is Completed.
[ OK ] Listening on standard Q&A socket.
[ OK ] Starting Update is Completed.
[ OK ] Reached ready mode.
[ OK ] Starting Update is Completed.
      Starting Audio Module...
      Starting Service enabling compressing RAM with zRam...
      Starting Hold until boot process finishes up...
[ OK ] Started Terminate all nervously influenced input channels.
[ OK ] Started Hold until boot process finishes up...
```

"Thema avond Mainframe Security" - Mainframe Meerwaarde

* Feedback: Yes please :)

* Contact me: <https://twitter.com/wizardofzos>
<https://nl.linkedin.com/in/wizardofzos>
<https://mainframesociety.com/users/7138614>

* Emails: wizard@zdevops.com
henri@mainframesociety.com

System information as of Thu 20 Nov 2025 10:00:38 PM UTC

Last login: Thu Nov 20 16:55:49 2024

[henri@palehoof](#):~\$ 

"Thema avond Mainframe Security" - Mainframe Meerwaarde

* Feedback: Yes please :)

* Contact me: <https://twitter.com/wizardofzos>
<https://nl.linkedin.com/in/wizardofzos>
<https://mainframesociety.com/users/7138614>

* Emails: wizard@zdevops.com
henri@mainframesociety.com

System information as of Thu 20 Nov 2025 10:00:38 PM UTC

Last login: Thu Nov 20 16:55:49 2024

[henri@palehoof](#):~\$ w

"Thema avond Mainframe Security" - Mainframe Meerwaarde

* Feedback: Yes please :)

* Contact me: <https://twitter.com/wizardofzos>
<https://nl.linkedin.com/in/wizardofzos>
<https://mainframesociety.com/users/7138614>

* Emails: wizard@zdevops.com
henri@mainframesociety.com

System information as of Thu 20 Nov 2025 10:00:38 PM UTC

Last login: Thu Nov 20 16:55:49 2024

[henri@palehoof](#):~\$ wh

"Thema avond Mainframe Security" - Mainframe Meerwaarde

* Feedback: Yes please :)

* Contact me: <https://twitter.com/wizardofzos>
<https://nl.linkedin.com/in/wizardofzos>
<https://mainframesociety.com/users/7138614>

* Emails: wizard@zdevops.com
henri@mainframesociety.com

System information as of Thu 20 Nov 2025 10:00:38 PM UTC

Last login: Thu Nov 20 16:55:49 2024

[henri@palehoof](#):~\$ who

"Thema avond Mainframe Security" - Mainframe Meerwaarde

* Feedback: Yes please :)

* Contact me: <https://twitter.com/wizardofzos>
<https://nl.linkedin.com/in/wizardofzos>
<https://mainframesociety.com/users/7138614>

* Emails: wizard@zdevops.com
henri@mainframesociety.com

System information as of Thu 20 Nov 2025 10:00:38 PM UTC

Last login: Thu Nov 20 16:55:49 2024

[henri@palehoof](#):~\$ [whoa](#) 

"Thema avond Mainframe Security" - Mainframe Meerwaarde

* Feedback: Yes please :)

* Contact me: <https://twitter.com/wizardofzos>
<https://nl.linkedin.com/in/wizardofzos>
<https://mainframesociety.com/users/7138614>

* Emails: wizard@zdevops.com
henri@mainframesociety.com

System information as of Thu 20 Nov 2025 10:00:38 PM UTC

Last login: Thu Nov 20 16:55:49 2024

[henri@palehoof](#):~\$ [whoam](#) 

"Thema avond Mainframe Security" - Mainframe Meerwaarde

* Feedback: Yes please :)

* Contact me: <https://twitter.com/wizardofzos>
<https://nl.linkedin.com/in/wizardofzos>
<https://mainframesociety.com/users/7138614>

* Emails: wizard@zdevops.com
henri@mainframesociety.com

System information as of Thu 20 Nov 2025 10:00:38 PM UTC

Last login: Thu Nov 20 16:55:49 2024

[henri@palehoof](#):~\$ [whoami](#) 

"Thema avond Mainframe Security" - Mainframe Meerwaarde

* Feedback: Yes please :)

* Contact me: <https://twitter.com/wizardofzos>
<https://nl.linkedin.com/in/wizardofzos>
<https://mainframesociety.com/users/7138614>

* Emails: wizard@zdevops.com
henri@mainframesociety.com

System information as of Thu 20 Nov 2025 10:00:38 PM UTC

Last login: Thu Nov 20 16:55:49 2024

[henri@palehoof](#):~\$ [whoami](#)



"Thema avond Mainframe Security" - Mainframe Meerwaarde

- * Feedback: Yes please :)
- * Contact me: <https://twitter.com/wizardofzos>
<https://nl.linkedin.com/in/wizardofzos>
<https://mainframesociety.com/users/7138614>
- * Emails: wizard@zdevops.com
henri@mainframesociety.com

System information as of Thu 20 Nov 2025 10:00:38 PM UTC

Last login: Thu Nov 20 16:55:49 2024

henri@palehoof:~\$ **whoami**

uid=1000(henri) gid=4(zdevops) groups=4(zdevops),22(mainframesociety),401(use),1047(ibmchampion),3270(zigi),4011(mfpandas)

henri@palehoof:~\$ █

"Thema avond Mainframe Security" - Mainframe Meerwaarde

- * Feedback: Yes please :)
- * Contact me: <https://twitter.com/wizardofzos>
<https://nl.linkedin.com/in/wizardofzos>
<https://mainframesociety.com/users/7138614>
- * Emails: wizard@zdevops.com
henri@mainframesociety.com

System information as of Thu 20 Nov 2025 10:00:38 PM UTC

Last login: Thu Nov 20 16:55:49 2024

henri@palehoof:~\$ whoami

uid=1000(henri) gid=4(zdevops) groups=4(zdevops),22(mainframesociety),
401(use),1047(ibmchampion),3270(zigi),4011(mfpandas)

henri@palehoof:~\$ r 

"Thema avond Mainframe Security" - Mainframe Meerwaarde

- * Feedback: Yes please :)
- * Contact me: <https://twitter.com/wizardofzos>
<https://nl.linkedin.com/in/wizardofzos>
<https://mainframesociety.com/users/7138614>
- * Emails: wizard@zdevops.com
henri@mainframesociety.com

System information as of Thu 20 Nov 2025 10:00:38 PM UTC

Last login: Thu Nov 20 16:55:49 2024

henri@palehoof:~\$ **whoami**

uid=1000(henri) gid=4(zdevops) groups=4(zdevops),22(mainframesociety),401(use),1047(ibmchampion),3270(zigi),4011(mfpandas)

henri@palehoof:~\$ **ru** 

"Thema avond Mainframe Security" - Mainframe Meerwaarde

- * Feedback: Yes please :)
- * Contact me: <https://twitter.com/wizardofzos>
<https://nl.linkedin.com/in/wizardofzos>
<https://mainframesociety.com/users/7138614>
- * Emails: wizard@zdevops.com
henri@mainframesociety.com

System information as of Thu 20 Nov 2025 10:00:38 PM UTC

Last login: Thu Nov 20 16:55:49 2024

henri@palehoof:~\$ **whoami**

uid=1000(henri) gid=4(zdevops) groups=4(zdevops),22(mainframesociety),401(use),1047(ibmchampion),3270(zigi),4011(mfpandas)

henri@palehoof:~\$ **run** 

"Thema avond Mainframe Security" - Mainframe Meerwaarde

- * Feedback: Yes please :)
- * Contact me: <https://twitter.com/wizardofzos>
<https://nl.linkedin.com/in/wizardofzos>
<https://mainframesociety.com/users/7138614>
- * Emails: wizard@zdevops.com
henri@mainframesociety.com

System information as of Thu 20 Nov 2025 10:00:38 PM UTC

Last login: Thu Nov 20 16:55:49 2024

```
henri@palehoof:~$ whoami
uid=1000(henri) gid=4(zdevops) groups=4(zdevops),22(mainframesociety),
401(use),1047(ibmchampion),3270(zigi),4011(mfpandas)
henri@palehoof:~$ run
```



Voor het geval je niet
weet wie ik ben...

Dit ben ik —>





Tax Administration



- henrikuiper@zdevops.com
- henri@mainframesociety.com
- github.com/wizardofzos
- www.linkedin.com/in/wizardofzos/
- <https://www.credly.com/users/wizardofzos/badges>

IBM
Champion
**7 Year
Milestone**

IBM

Awarded through the program

IBM Champion





Mijn 1ste computer...

Mijn tweede...

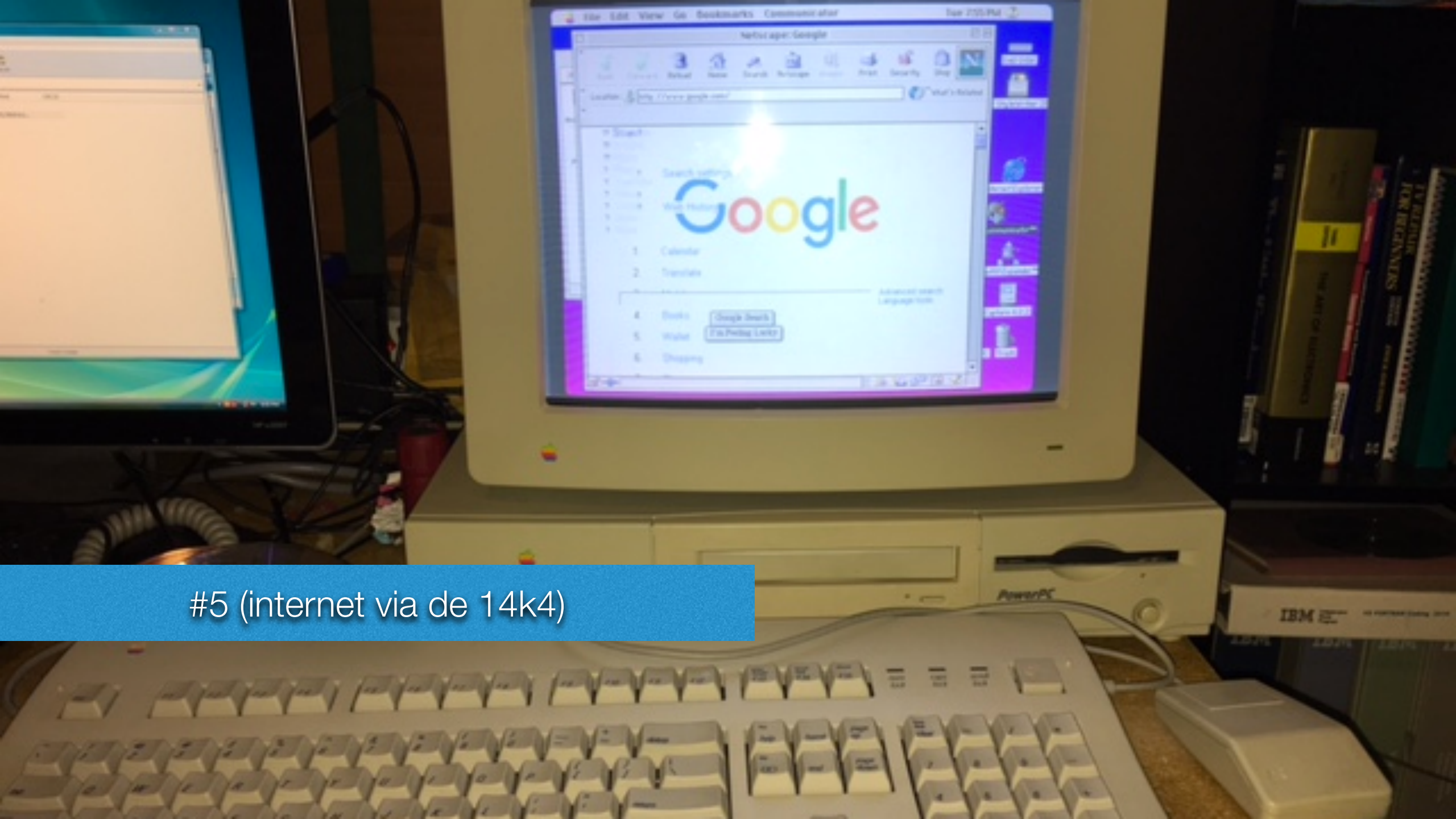




Derde...

Nummer 4





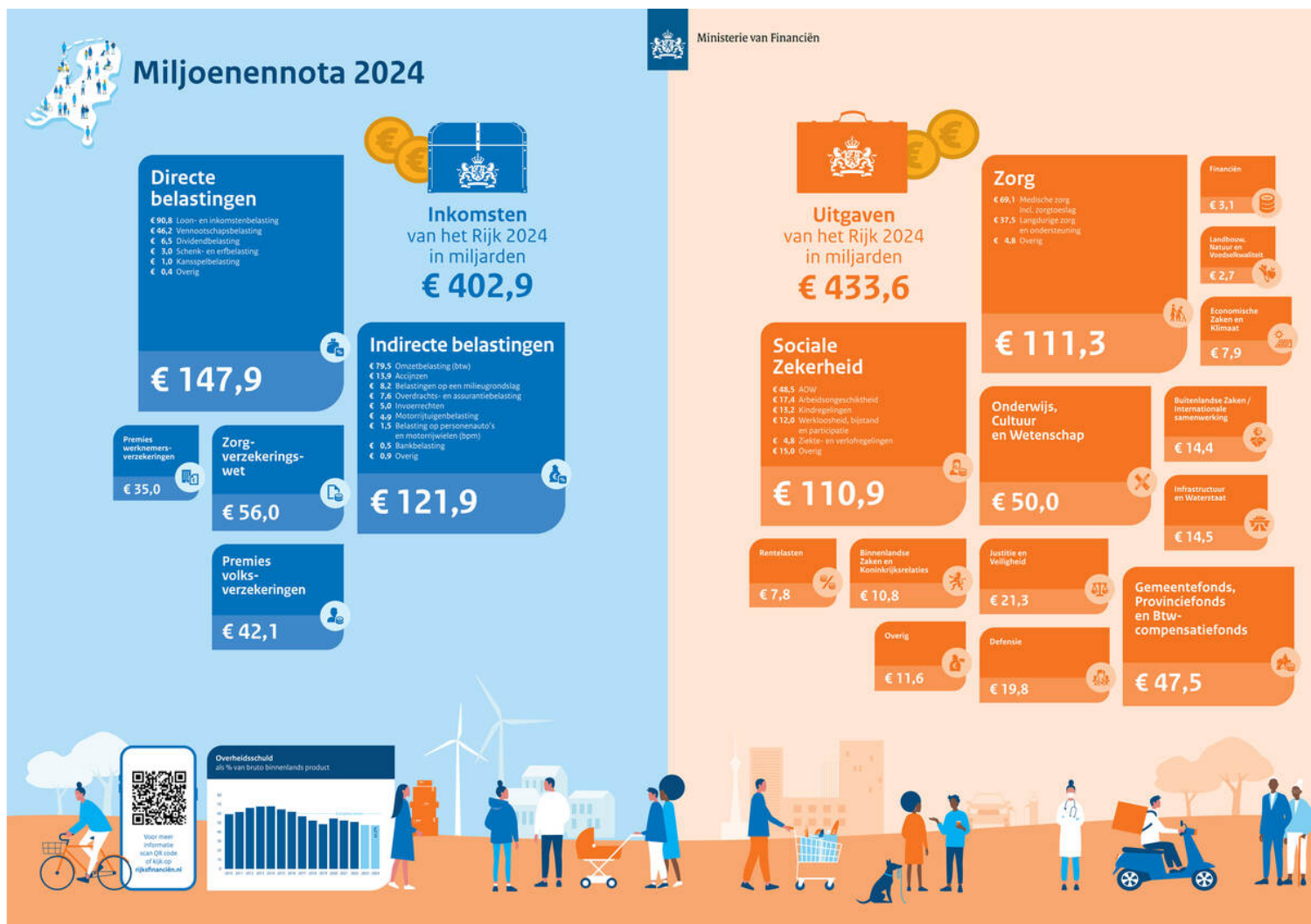
#5 (internet via de 14k4)



Mijn favoriete computer



206x 5.5Ghz. CPU
60TB Geheugen
Telum II, Spire
Massive I/O
 2.4×10^{13} OP/s
IBM z17



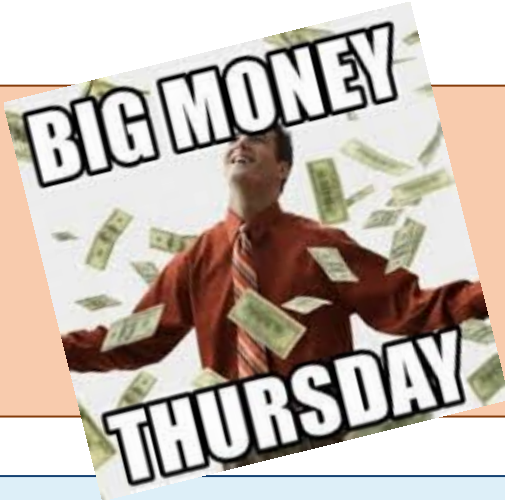
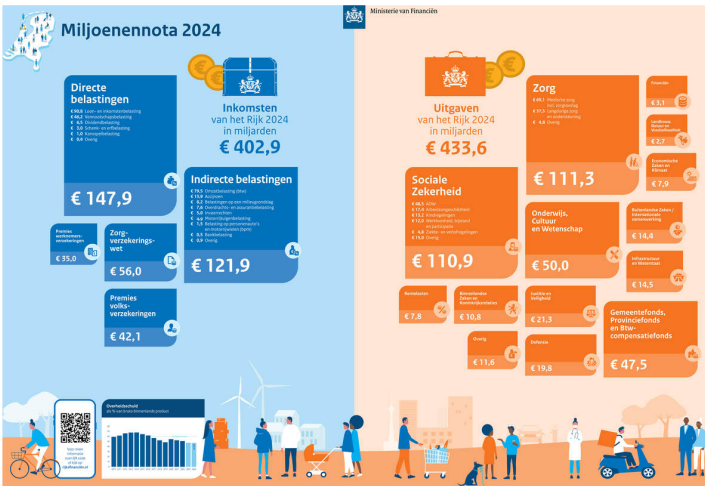
Belastingdienst - Toeslagen - Douane

(de “Mainframe Workload” = plm. 70%)



Kerngetallen per maand:

- COBOL transacties: **416 Miljoen**
- Backend jobs: **240K**
- Java verzoeken: **135 Miljoen**
- CPU: **3000 uur**



High Available “Active-Active”
(GDPS-Technologie met HyperSwap)

Stroomverbruik

40 KW

Opslag

6.7 PB

Tape (~50% utilisatie, compressie ~3:1)

1.2 PB

Disk (~70% utilisatie)

CPU's

18

CCD

19

JAVA

46

zLinux / BPM

Locatie-1

Memory

16,5 Terabyte

40 KW

Stroomverbruik

1.2 PB

Disk (~70% utilisatie)

6.7 PB

Tape (~50% utilisatie, compressie ~3:1)

CPU's

46

zLinux / BPM

19

JAVA

18

CCD

16,5 Terabyte

Memory

Locatie-2

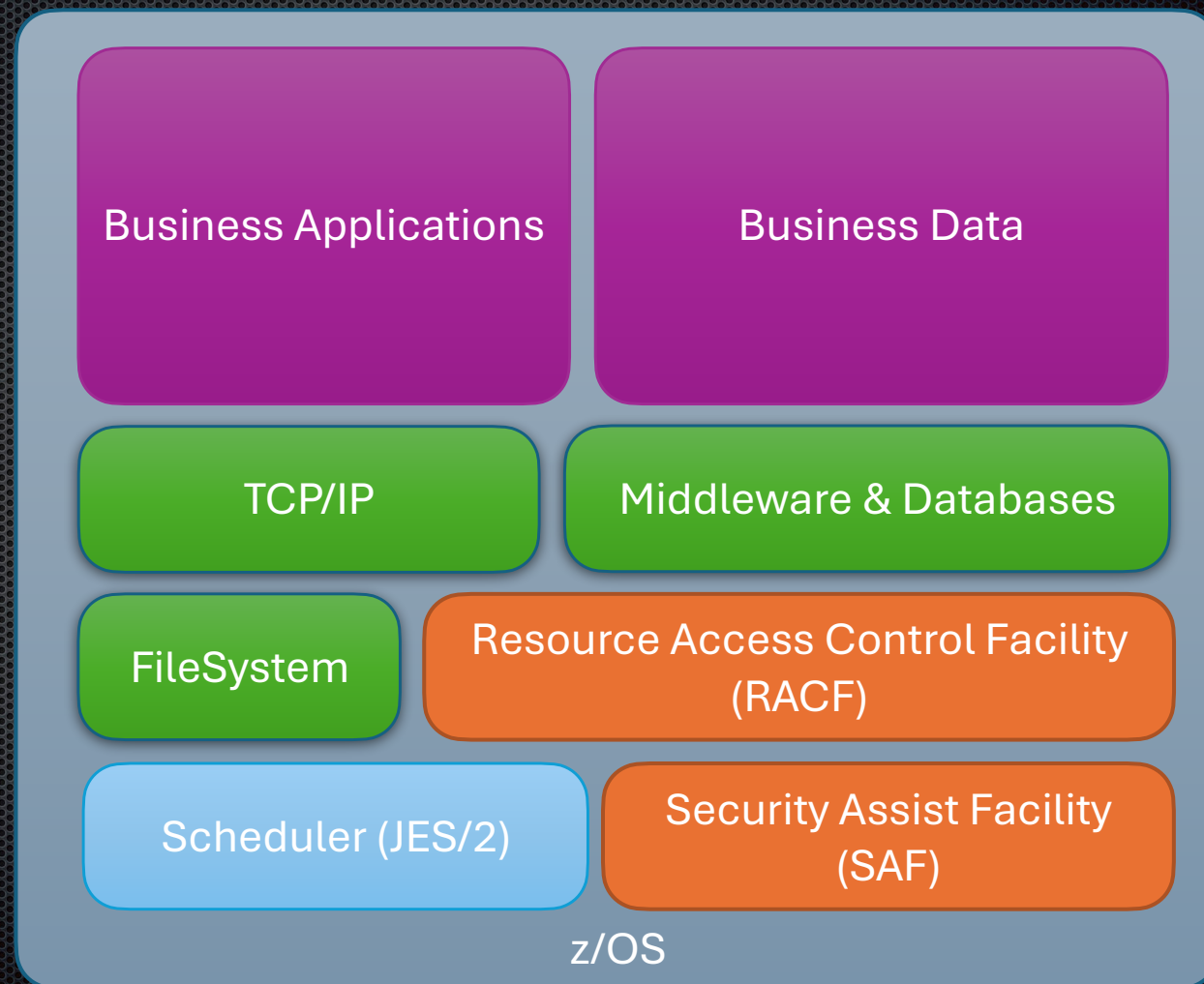
Mainframe Security Bootcamp

Audience Participation Moment

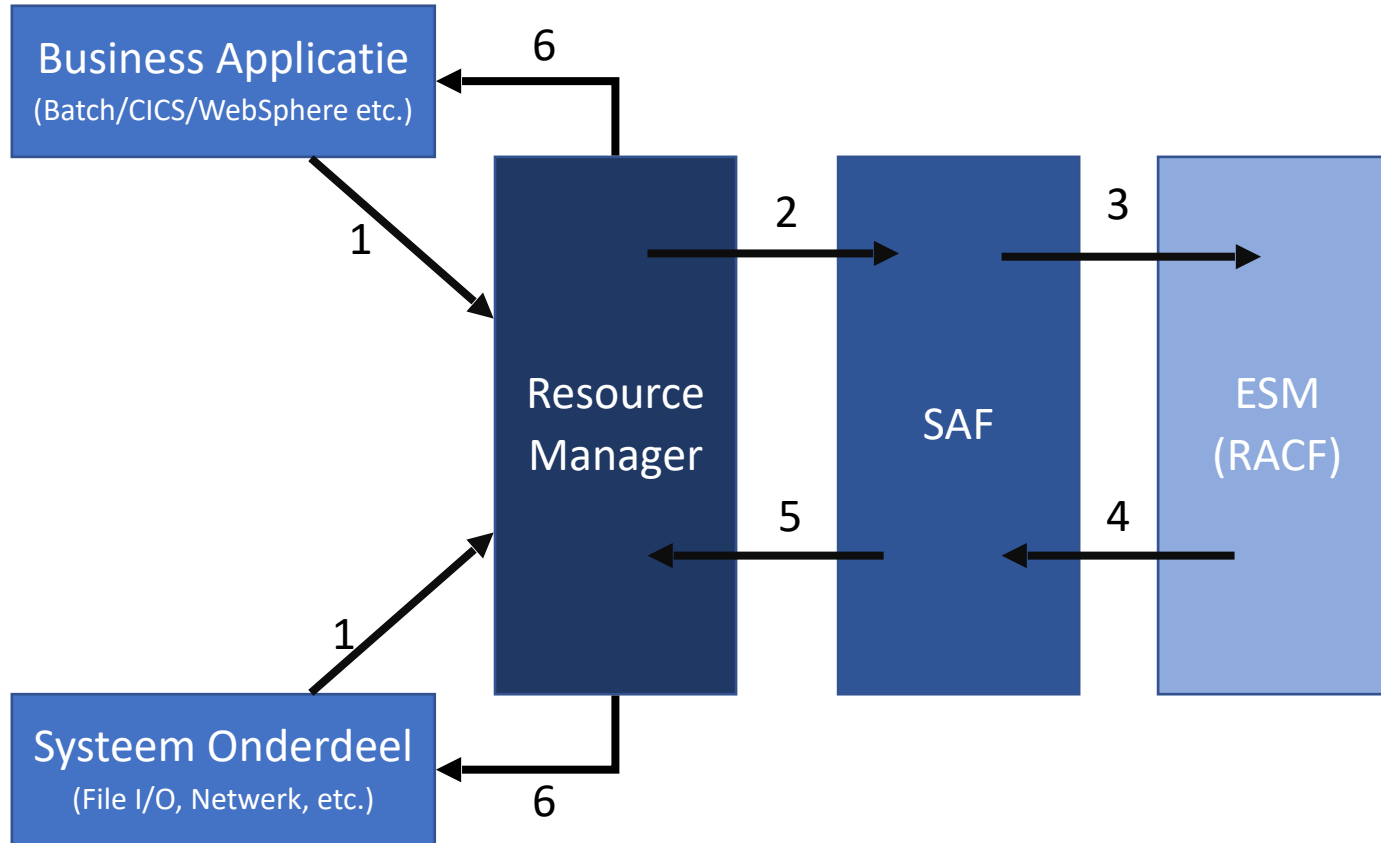




z/OS (Simplified!)



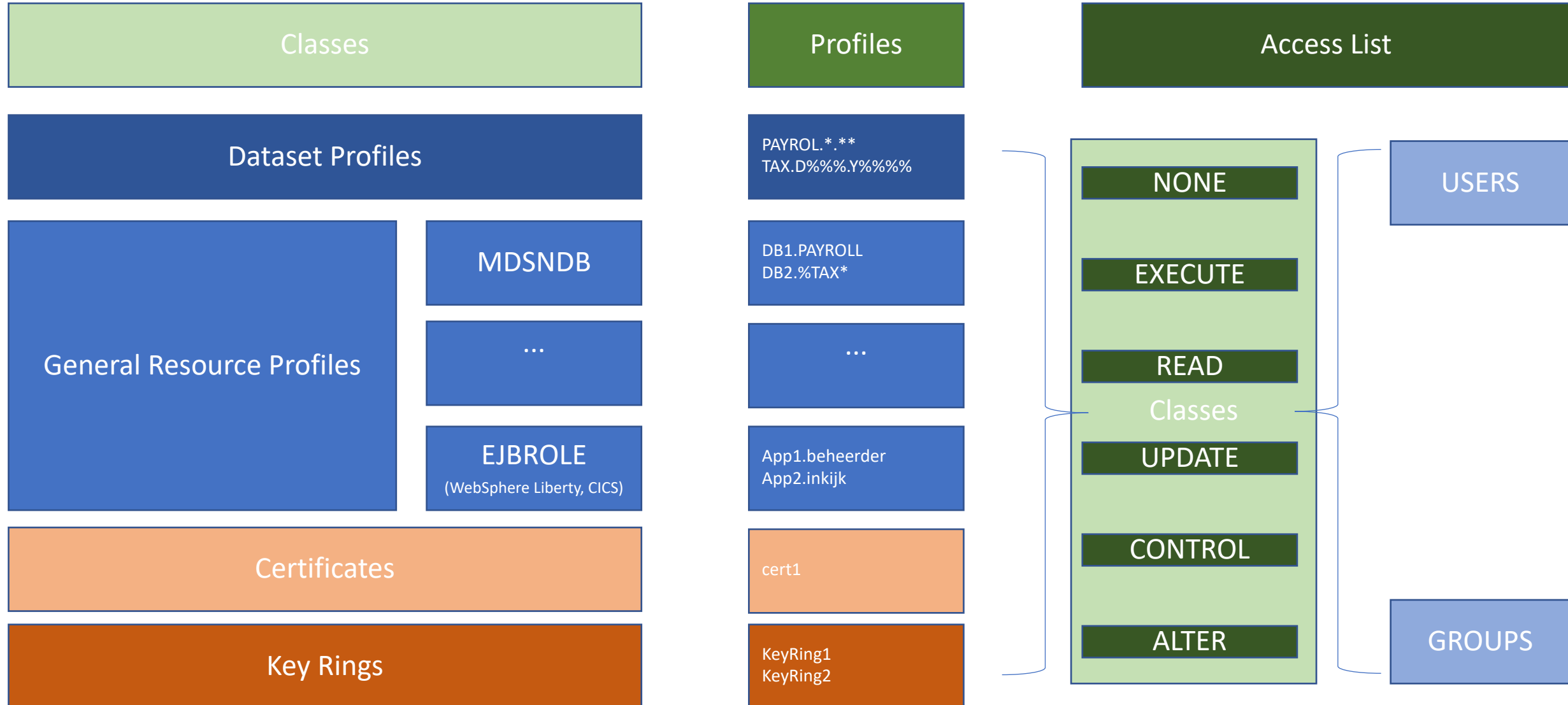
Hoe beveiligen we dat?: Autorisatie flow z/OS



1. Usercontext (UserID en groepen) worden door applicatie of systeem component naar de resource manager doorgegeven met de vraag “mag de user dit?”
2. De resource manager bepaalt het toegangsprofiel waar de user toegang toe moet krijgen en vraagt aan SAF of de user hier het juiste access level toe heeft
3. SAF geeft de usercontext, de resource en het gewenste access level door aan de ESM (RACF, TopSecret, ACF2) met de vraag of de user hierbij mag
4. ESM kijkt in de database of de user het juiste access level heeft en geeft dit terug aan SAF
5. Via SAF krijgt de Resource Manager dit antwoord in het formaat “Mag, Mag niet of Weet niet”
6. Op basis van dit antwoord besluit de Resource Manager of de user toegang krijgt of niet (ICH408I)

SAF: System Authorisation Facility, **ESM:** External Security Manager, **RACF:** Resource Access Control Facility

Layout van de RACF Database



Wat betekenen die access levels?

NONE	Totaal geen toegang
EXECUTE	Executables uitvoeren maar niet inzien
READ	Lezen
UPDATE	Lezen, Aanpassen/Opslaan
CONTROL	Access to VSAM dataset control
ALTER	Maken, Lezen, Aanpassen/Opslaan, verwijderen, hernoemen

- Dit is de betekenis voor profielen binnen de **DATASET** class
- Voor andere classes is soms alleen READ nodig om de 'functionaliteit' te gebruiken (denk aan EJBROLES)
- Het verschilt dus *per class, per Resource Manager* wat het effect van het access level is
- Soms resulteerd een 'weet niet' in een 'doe dan maar'
- "Redelijke" kennis van de applicatie of systeem component is derhalve vereist voor een juiste beoordeling van het accesslevel en een veilige inrichting

Auditing & Control Capabilities

- Logging van FAIL
- Logging van SUCCESS
- Wie mag wanneer bij welke resource?
- Etc. etc.

DATASETS

HENRI.SOMEQUAL.OTHER.FILE

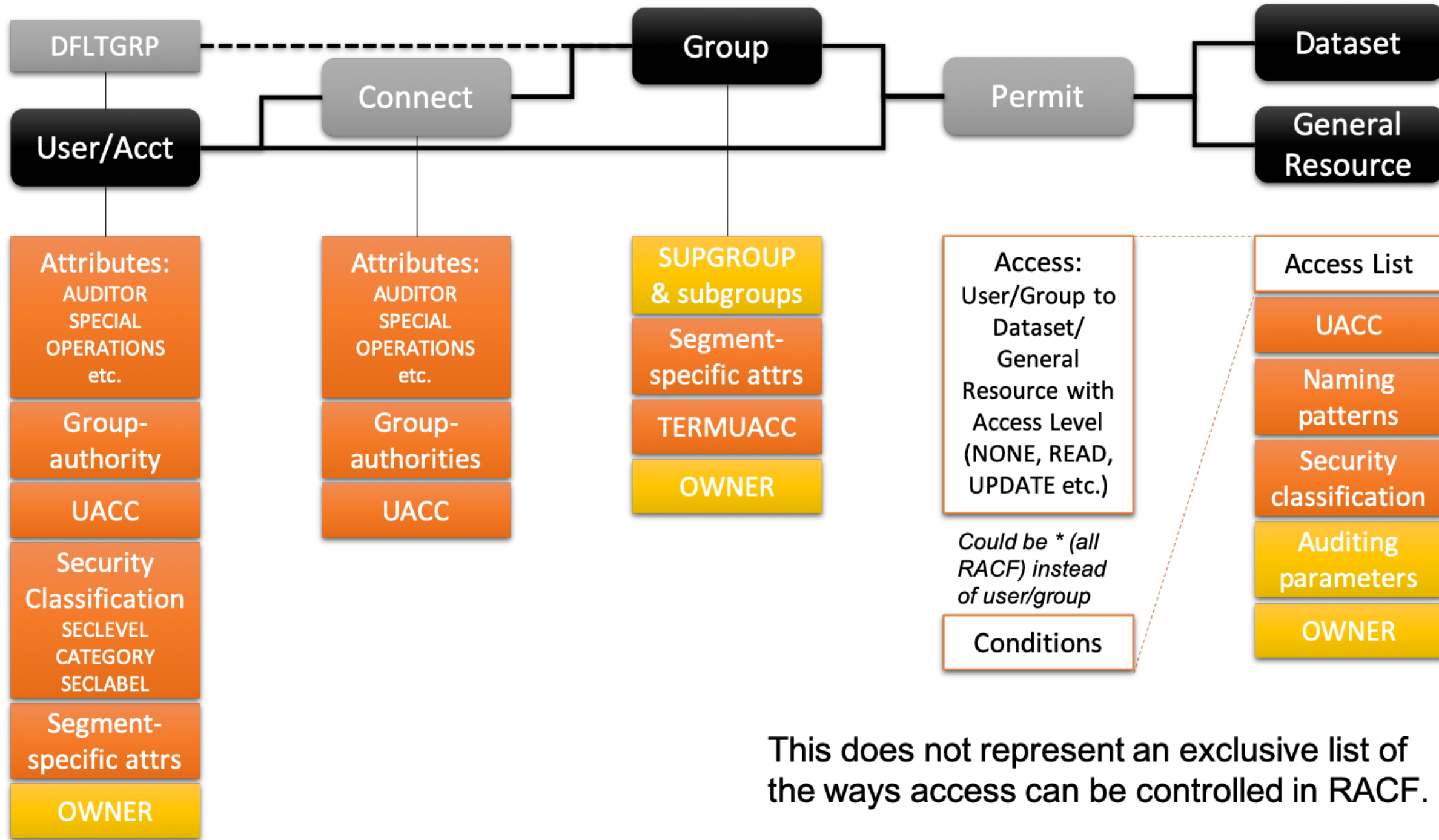
High Level Qualifier
(HLQ)

Low Level Qualifier
(LLQ)

MAX LENGTH: 44 (including the dots)

MAX QUALIFIER LENGTH: 8

QUALIFIERS START: A-Z #@\$



This does not represent an exclusive list of the ways access can be controlled in RACF.



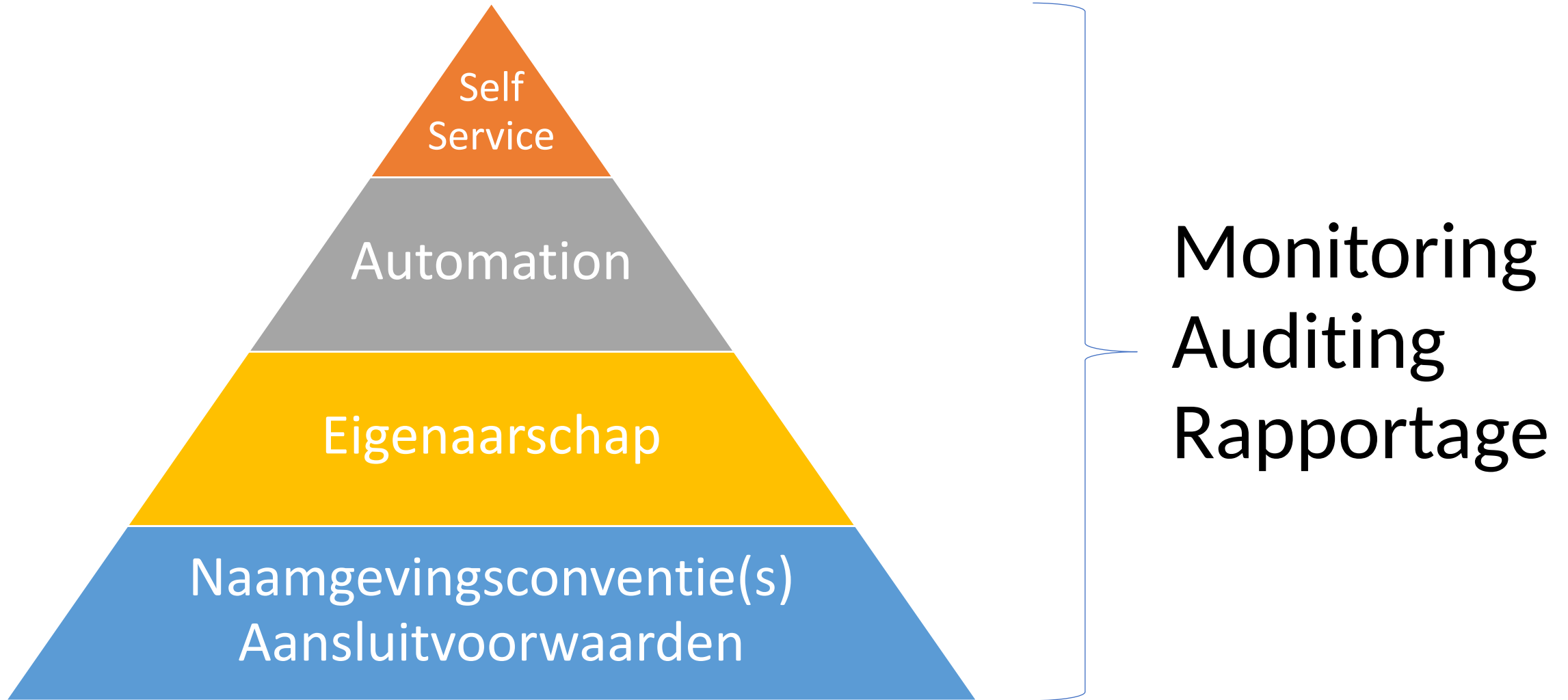
z/os

A man with dark hair and light-colored eyes, wearing a black hooded sweatshirt, is looking directly at the camera. The text 'z/os' is superimposed over the image, with the 'z' and '/' in a bold, sans-serif font, and the 'o' and 's' in a larger, more stylized font. The 'o' is partially obscured by the man's head.

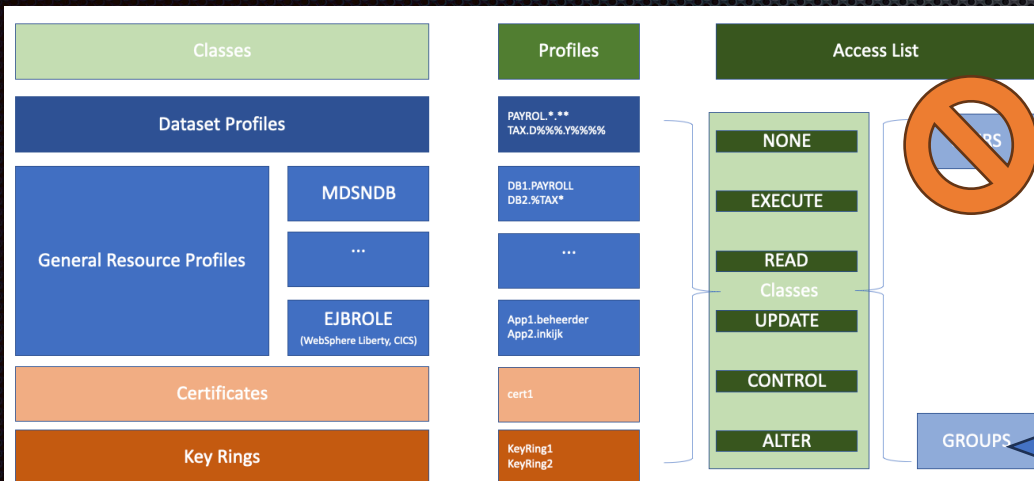
Just another operating system



Hoe is dat dan te beheren...



RBAC



Accounts krijgen uitsluitend toegang via *groepslidmaatschap*

Deze groepen zijn gekoppeld aan een (of meerdere) rollen

Roltoewijzing resulteert in groepslidmaatschap

En dus tot toegang tot resource profielen

GROUP1

Role2

GROUP2

Role1

GROUP3

NONE

EXECUTE

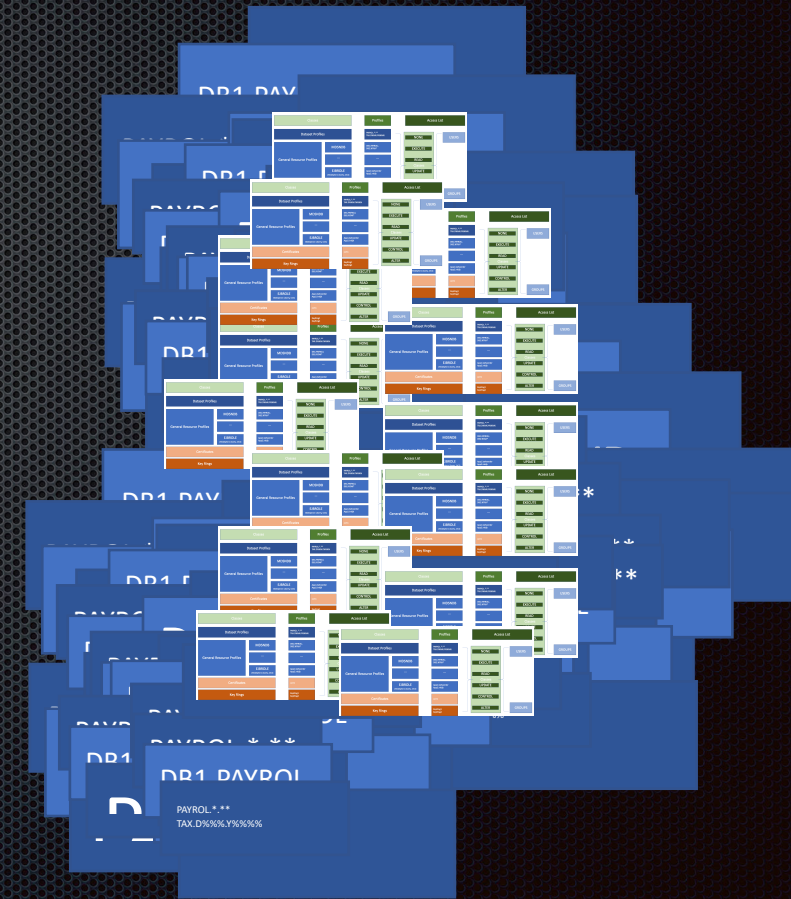
READ

Classes

UPDATE

CONTROL

ALTER



Self Service for RACF (REST API)



Python Application
Under 6000 lines of python (exluding frameworks)

Gunicorn

OMVS

User Management	
GET	/v1/Password
PUT	/v1/Password
PUT	/v1/Resume
GET	/v1/User
DELETE	/v1/User
GET	/v1/Users
Group Management	
POST	/v1/Connect
DELETE	/v1/Connect
GET	/v1/Group
DELETE	/v1/Group
GET	/v1/Groups
Dataset Management	
GET	/v1/Dataset
POST	/v1/Dataset
DELETE	/v1/Dataset

IronStream



Client Applications



RACF, JES/2, TCP/IP and all that good jazz

z/OS 3.1

THANK YOU



Henri Kuiper

@henrikuiper

Follow



I'm not saying let's
go kill all the stupid
people...I'm just
saying let's switch
all The Mainframes
off for a day and
see how stupid
they really are.....

someecards
user card



LIKES

3



12:44 AM - 12 Apr 2017



3