LA SÉCURITÉ DES SYSTÈMES MAINFRAMES

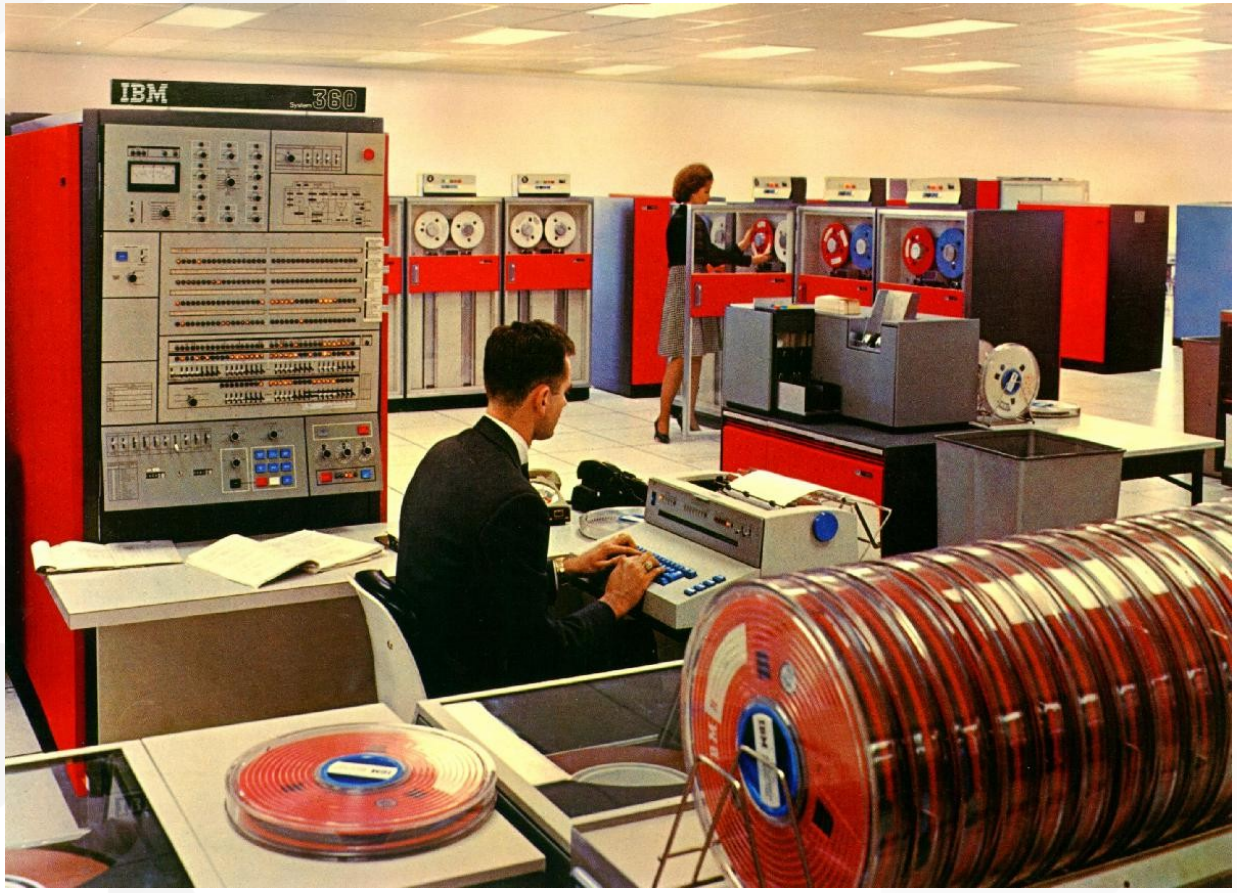
Stéphane Diacquenod

VOLVO IT

Sommaire

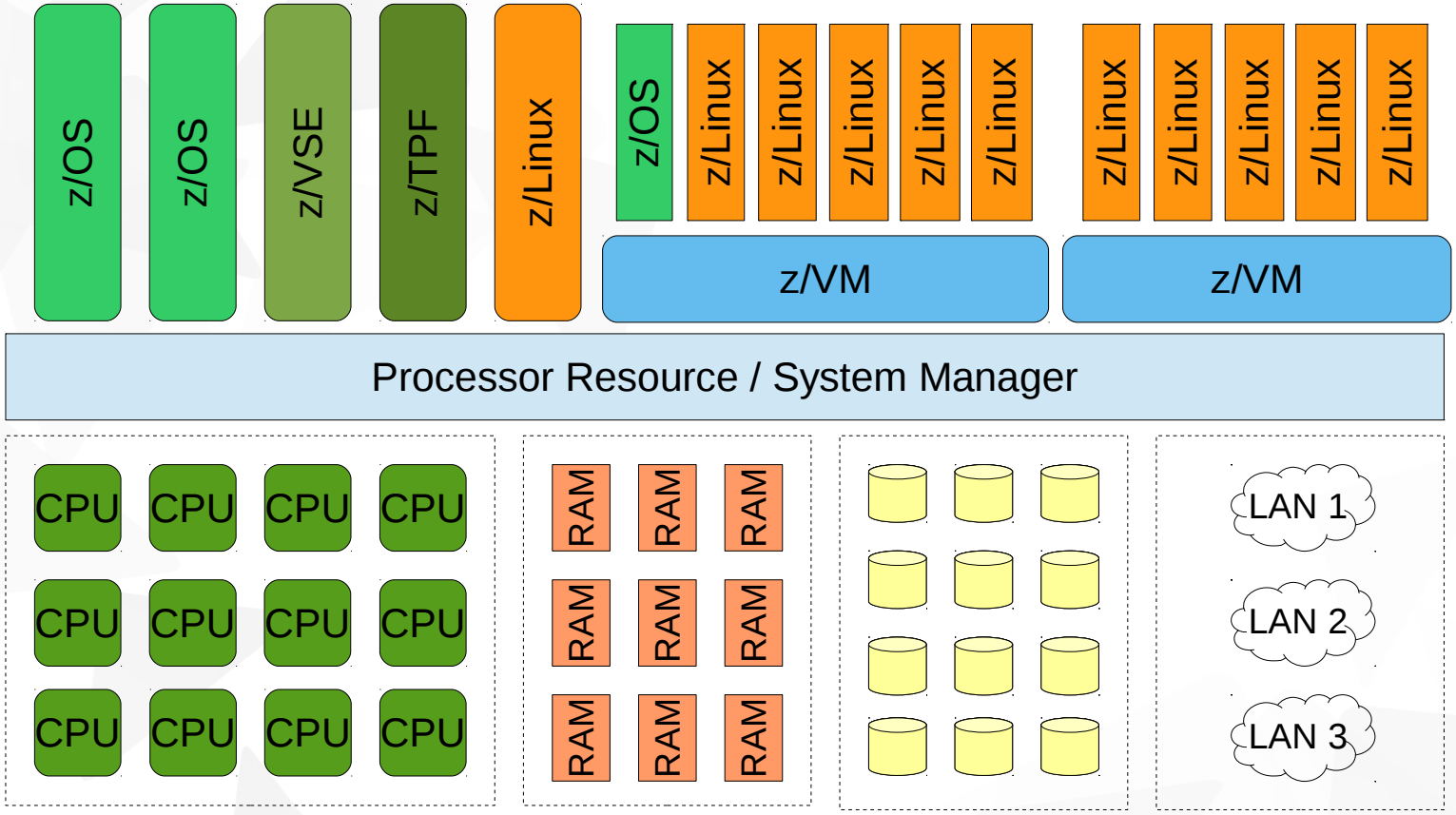
- Le mainframe
- L'architecture de z/OS
- Le contrôle d'accès
- Le multi-tâche

Le mainframe : System/360

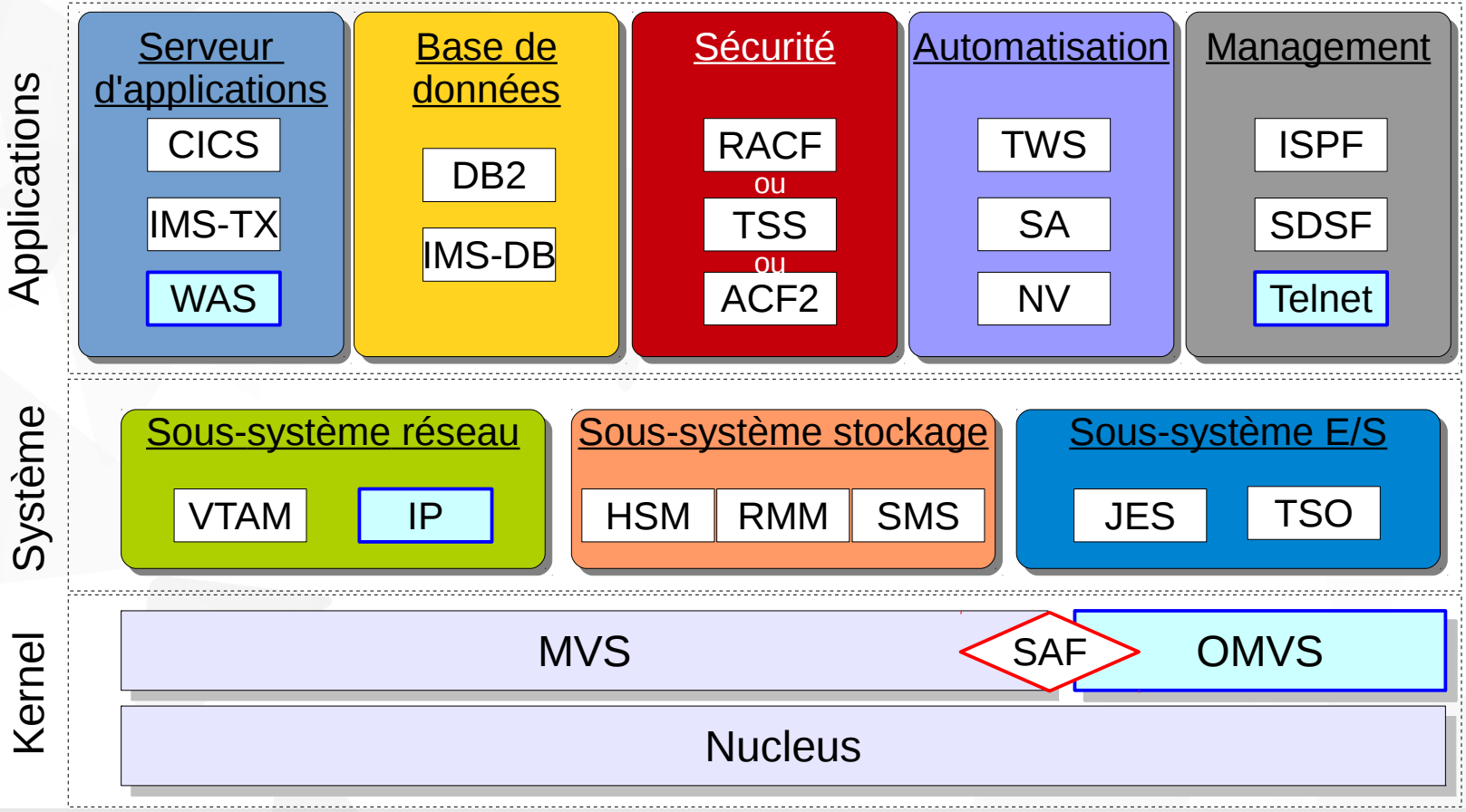


Le mainframe : zEntreprise EC12

Le mainframe : l'hyperviseur

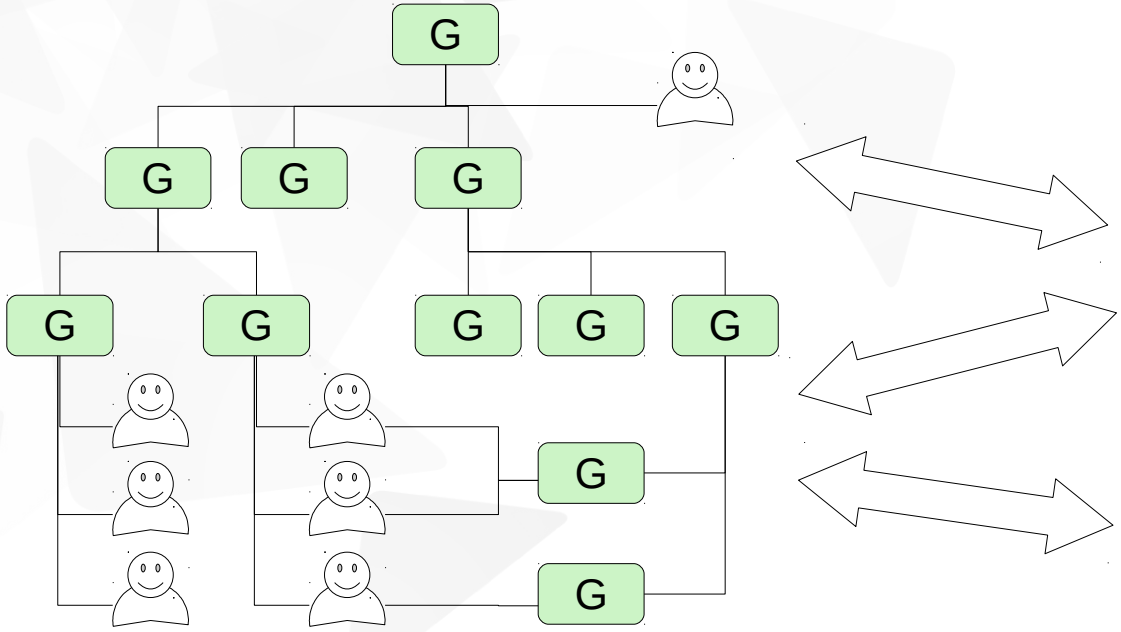


L'architecture de z/OS



Le contrôle d'accès : RACF

- Arborescences de droits RACF



- Ressources SAF

Resources class (z/OS)

R R R R R R R R R

Resources class (z/OS)

R R R R R R R R

Resources class (DB2)

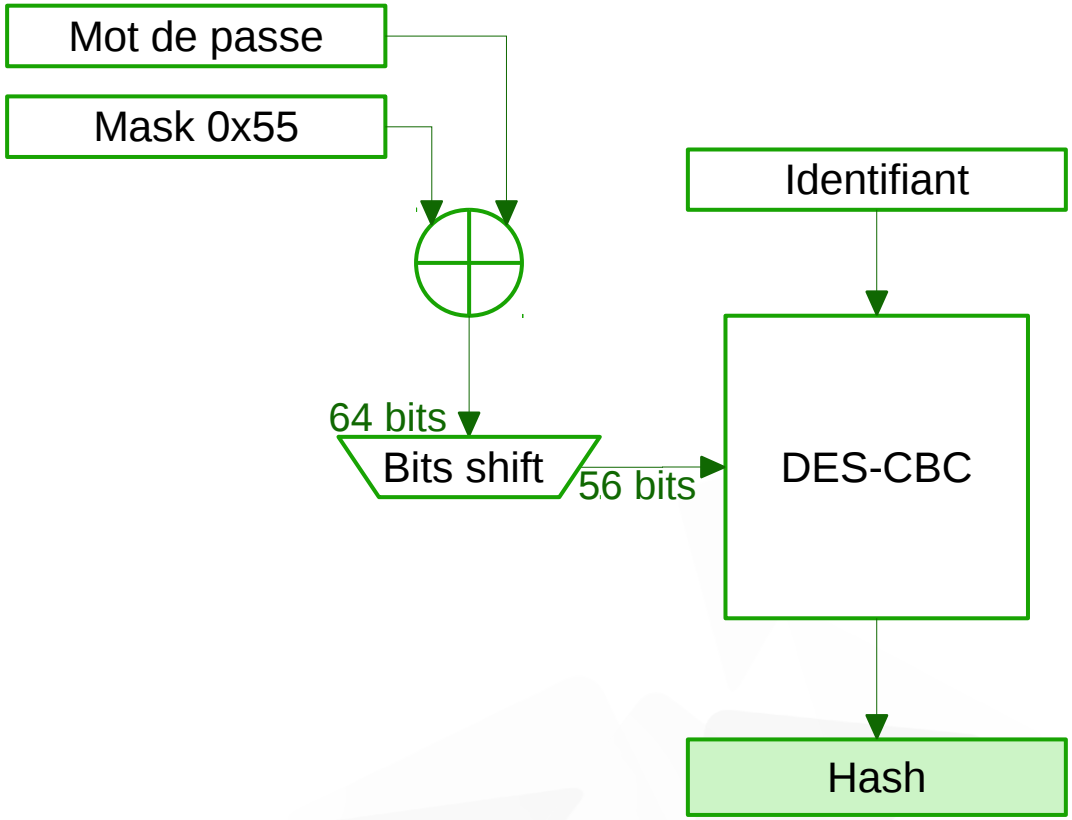
R R R R R R R R

Resources class FACILITY

R R R R R

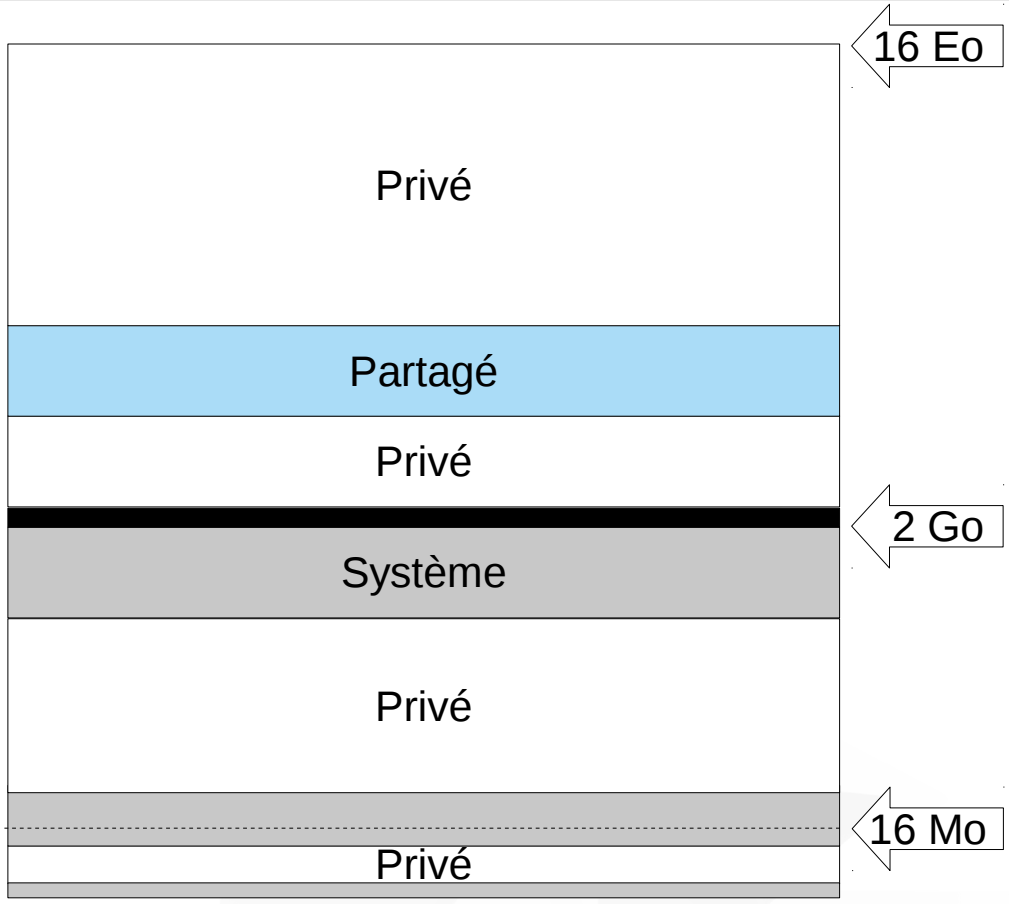
Le contrôle d'accès : mot de passe

- Mot de passe
  - Jusqu'à 8 caractères
  - non sensible à la casse (defaut)
  - Pas de ponctuation, speciaux
  - Caractère nationaux
    - # @ $ → £ à $
- Stockage
  - Algorithme non standard
  - Pas de *salt*
  - Sécurité faible : DES

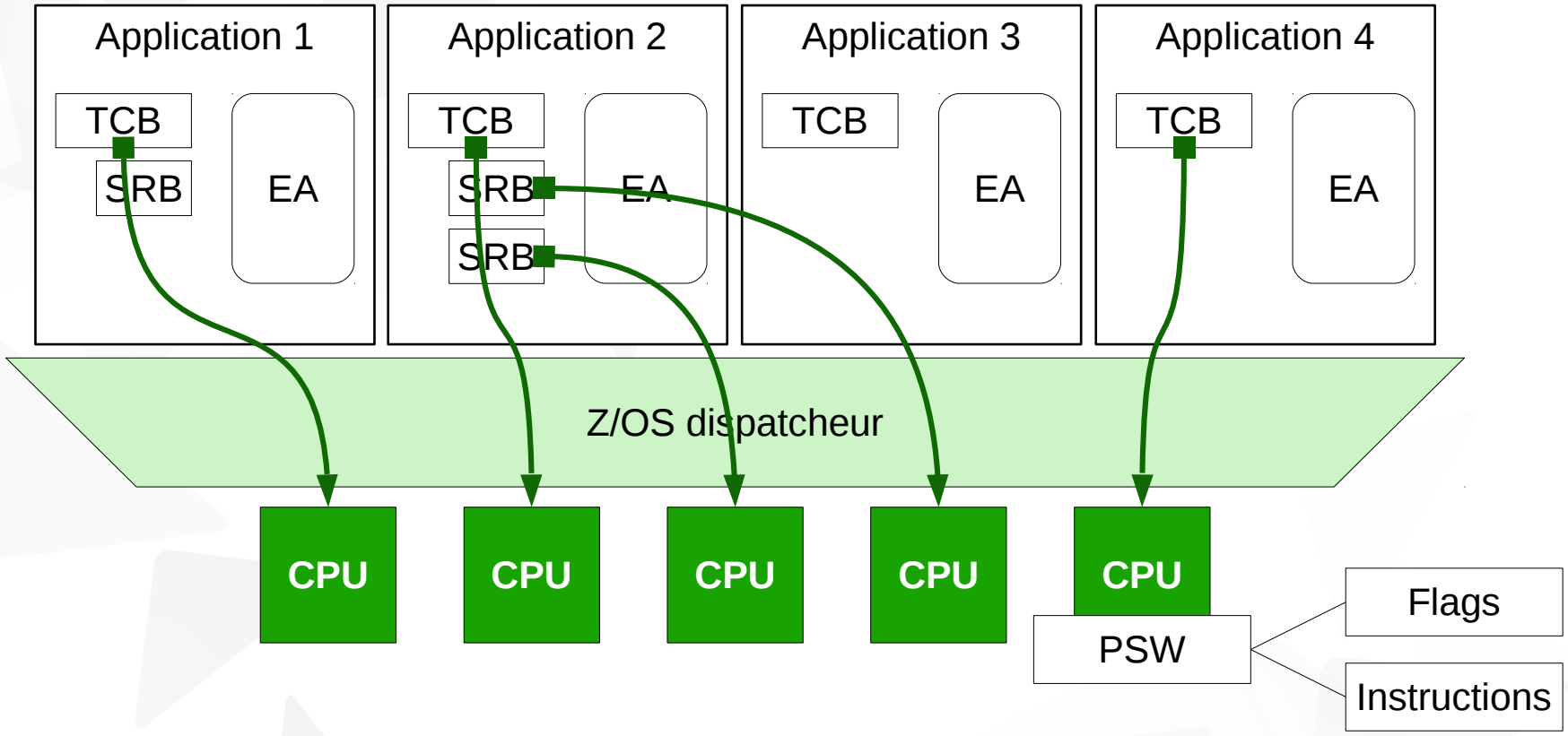


Sécurité du z/OS : la gestion du multi-tâche

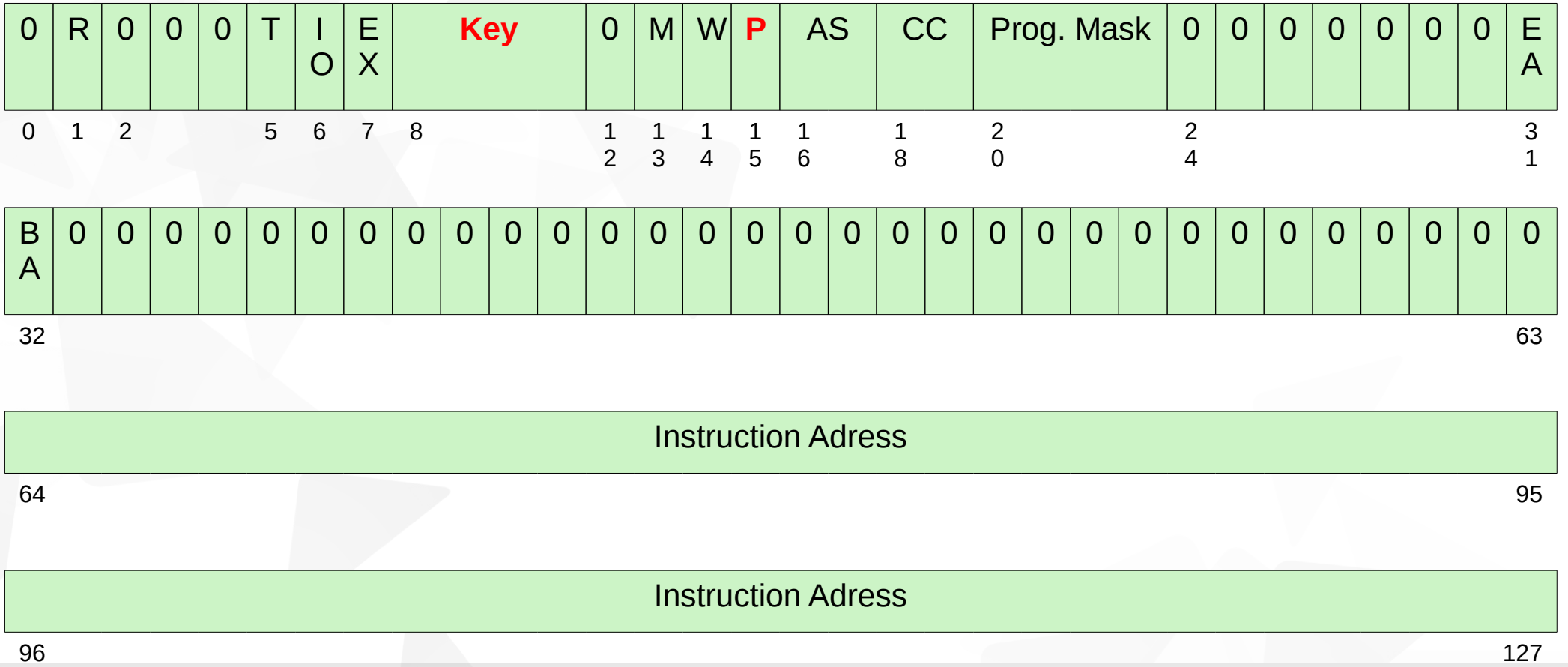
- Application :
  - Espace d'adressage
    - Zones privées (application)
    - Zones partagées (système)
  - Fil d'exécution
    - TCB → Processus
    - SRB → Thread



Sécurité du z/OS : la gestion du multi-tâche



Sécurité du z/OS : Program Status Word

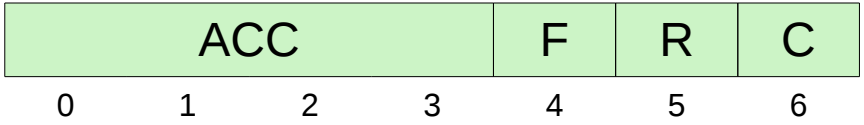


Sécurité du z/OS : APF

- Exécutions d'instructions privilégiées
  - Passage du processeur du mode problème au mode superviseur
  - Edition des liens du module avec l'option AC(1)
  - Déclaration de la bibliothèque dans l'APF
    - Authorized Program Facility
- Le contrôle des bibliothèques en APF est crucial

Sécurité du z/OS : pages mémoire

- Protection des pages mémoire
  - 16 clés de protection sont définies (0-F)
  - Le mécanisme vise à protéger les composants système.
  - Comparaisons de la clé du PSW et de la page



ACC : Access-control bits (0-F)
F : Fetch protection bit
R : Reference bit
C : Change bit

Comparaison des clés	Fetch protection bit	Accès en lecture	Accès en écriture
Clé identique	x	Oui	Oui
Clé différente	0	Oui	Non
	1	Non	Non

Sécurité du z/OS : pages mémoire

Key	Fonction
0	Clé « superviseur », accès à toutes les pages mémoire
1	Sous-système entrée / sortie (TSO, JES, TWS, ...)
2	*Réservé*
3	Availability manager (AVM)
4	*Réservé*
5	Sous-système stockage (SMS, HSM, RMM)
6	Sous-système réseau (VTAM, TCP/IP)
7	Midleware et Base de données (CICS, IMS, DB2, MQ)
8-9	Programmes utilisateurs en mémoire virtuelle
A-F	Programmes utilisateurs en mémoire réelle (une clé par programme)

Conclusion

Merci de votre attention