



# Unidade 3

## Conceitos básicos de Segurança

**Prof. Aparecido V. de Freitas**  
**Doutor em Engenharia da Computação pela EPUSP**





# Visão geral de Segurança

- Integrada com o IBM i
  - Security
  - Como DB2 for IBM i
- Acesso seguro ao sistema através de:
  - User sign-on
  - Menu
  - Hierarquia na classificação do Usuário
    - » Limiting capability



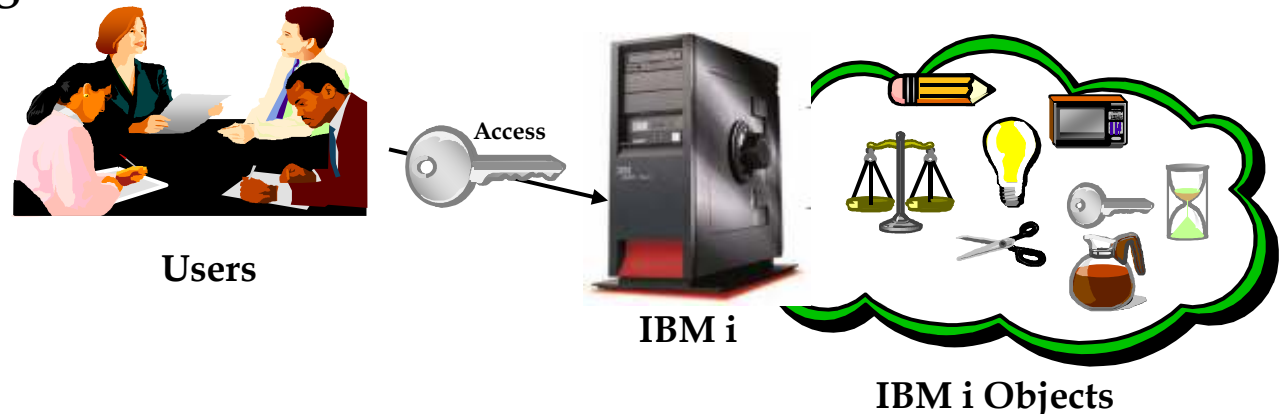
# Object security

- **Segurança de objetos individuais**

- Bibliotecas
- Database
  - » Physical
  - » Logical
- Programs/commands
- Devices

- **Accessibility by user**

- Object owner
  - » Authority to grant access





# Security System Values

Name in iSeries Navigator	Description of system value	Name in character-based interface
<a href="#">Security level</a>	Sets the level of security for your system.	QSECURITY
<a href="#">Allow server security information to be retained</a>	Sets server security information to be retained.	QRETSVRSEC
<a href="#">Users who can cause programs to use adopted authority from calling programs</a>	Specifies which users can work with programs with adopted authorities.	QUSEADPAUT
<a href="#">Default authority for newly created objects in QSYS.LIB file system</a>	Specifies the default authority for objects that do not specify the authority.	QCRTAUT
<a href="#">Allow use of shared or mapped memory with write capability</a>	Specifies whether users are allowed to use shared memory or mapped memory stream files or not.	QSHRMEMCTL
<a href="#">Allow these objects in . . .</a>	Specifies where to allow user domain objects that bypass authority checking and cannot be audited.	QALWUSRDMN
<a href="#">» Use registered exit programs to scan the root (/), QOpenSys, and user-defined file systems</a>	Specifies whether to scan file systems or not.	QSCANFS«
<a href="#">» Scan control</a>	Specifies scan control options.	QSCANFSCTL«





# Security System Value

- São variáveis do sistema para configurar o ambiente
- Algumas são efetivadas após o **IPL**
- São modificadas através do comando **CHGSYSVAL**
- São vistas através do comando **DSPSYSVAL**





# System Value

**QSECURITY: 10/20/30/40/50**

- 10 Não requer um Userid
- 20 Requer um Userid e uma Password
- 30 Acesso aos objetos depende de autoridade
- 40 Proteção à integridade do sistema
- 50 Checagem avançada de integridade do sistema





## System Value - Exemplo

**QMAXSIGN: 1-25**

**\*NOMAX**

**15**

- Define o número máximo de tentativas de Sign On
- Usuário pode ficar em estado \*DISABLED





# User Profiles

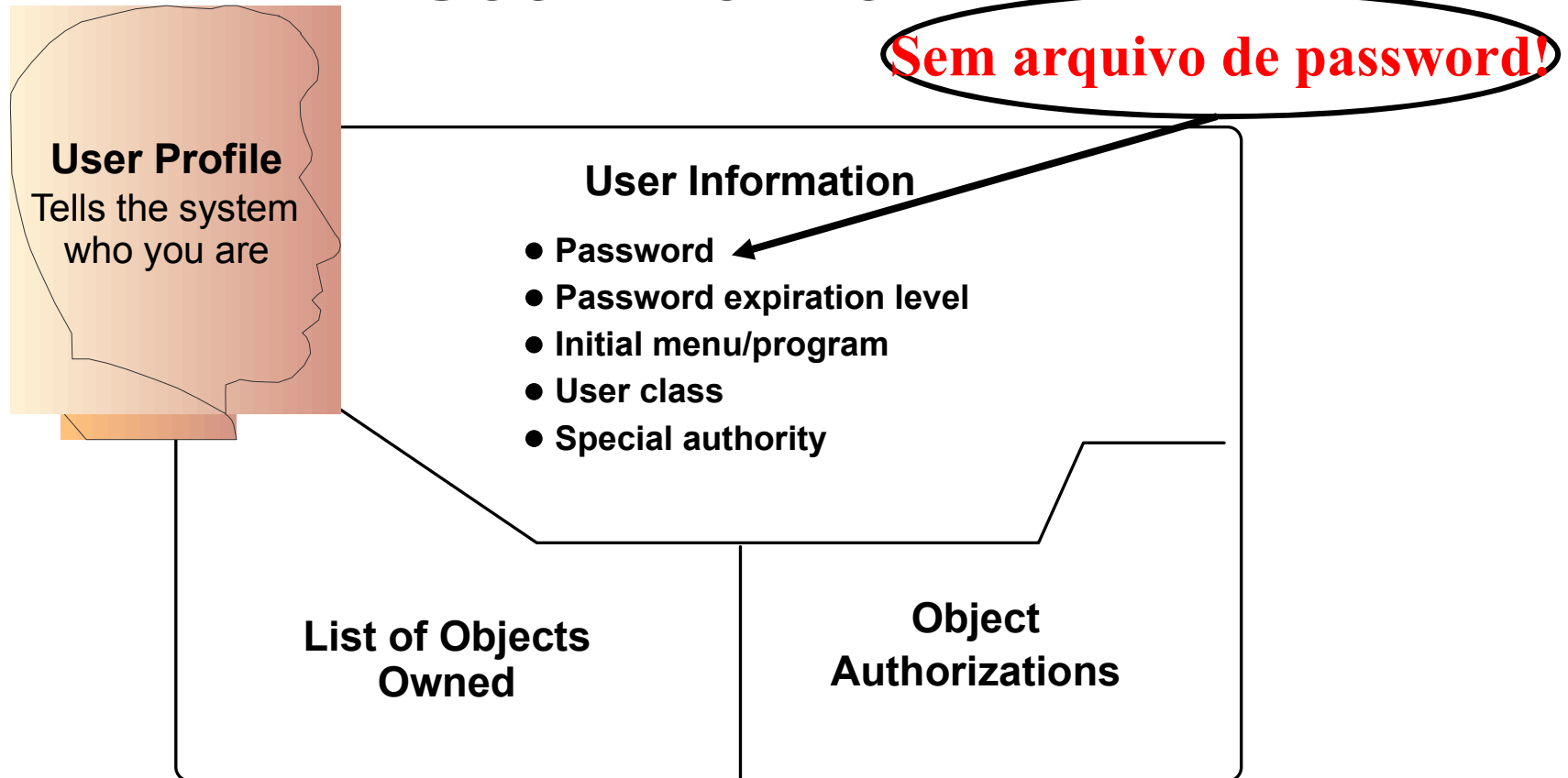
- Identificam os usuários no Sistema
- Informam ao Sistema as funções que o usuário pode acessar
- Definem as autorizações sobre os objetos
- São criadas através do comando **CRTUSRPRF**







# User Profile

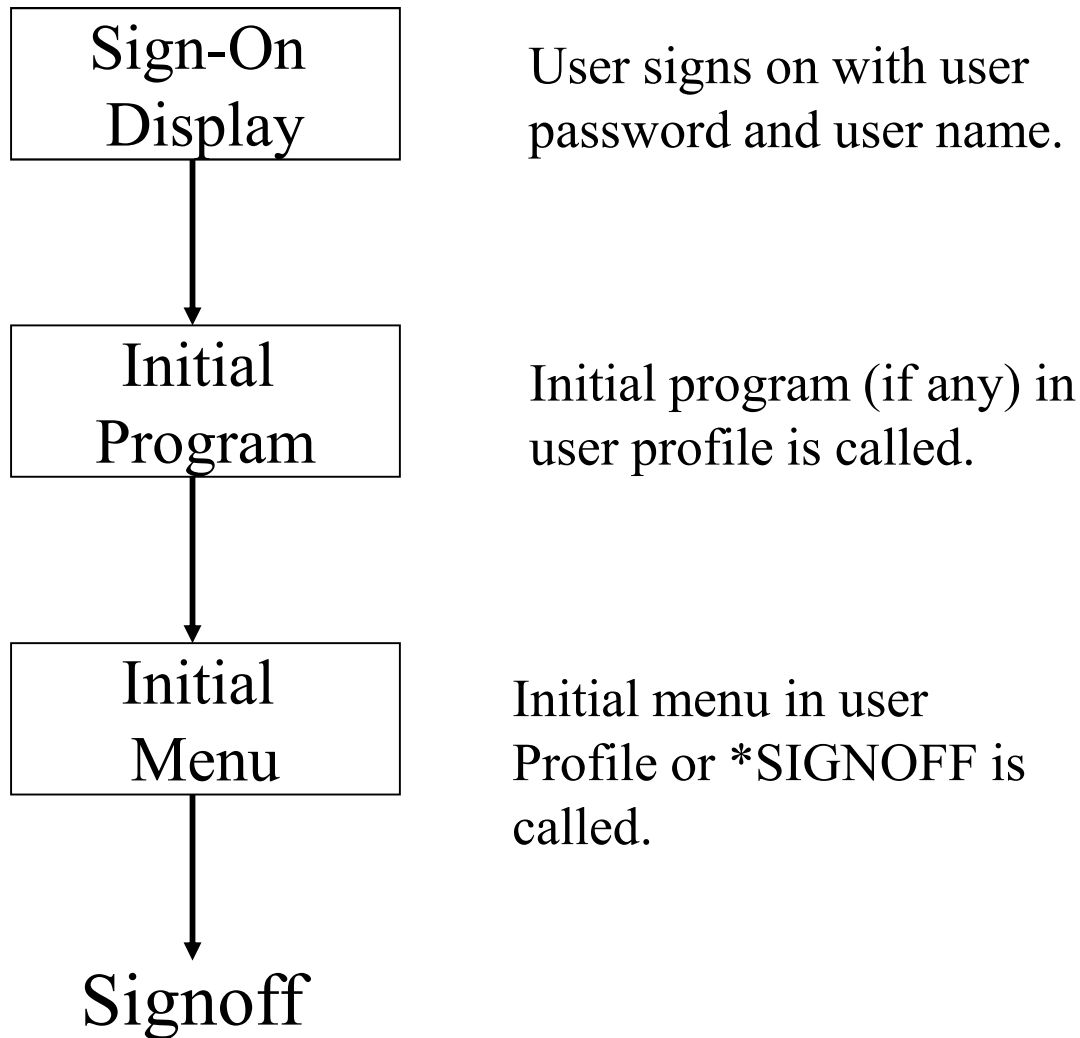


- iSeries Navigator: under Users and Groups
- DSPUSRPRF USRPRF(USERxx) TYPE(\*OBJOWN)  
or TYPE(\*OBJAUT)





# Initial Program e Menus





# IBM Supplied User Profiles

User profile	Privilege Classes
QSECOFR	Security officer
QPGMR	Programmer
QSYSOPR	System operator
QUSER	User
QDFTOWN	User
QSRV	Programmer
QSRVBAS	Programmer





# Tipos de Autoridades

## • **AUTORIDADE ESPECIAL**

- Definida na User Profile
- Identificada através da Classe do Usuário

## • **AUTORIDADE ESPECÍFICA**

- Define como o usuário pode acessar um objeto
- Autoridade a objetos
- Autoridade a dados





# Autoridade Especial

- \* **ALLOBJ** Acesso a todos os recursos do sistema
- \* **SECADM** Define e modifica User Profiles
- \* **SAVSYS** Operações de Save e Restore p/todo o sistema
- \* **JOBCTL** Manipula Job Queues e Subsistemas
- \* **SPLCTL** Controle de funções de Spool
- \* **SERVICE** Funções de Serviço





## Autoridade Específica Definida pelo sistema

- \***ALL** Todos os privilégios ao Objeto e aos Dados
- \***CHANGE** Privilégio de operar o Objeto e todos os privilégios para os Dados
- \***USE** Permissão para leitura dos dados
- \***EXCLUDE** Nenhuma autoridade sobre o objeto





## Comandos CL p/tratamento da Segurança

- **EDTOBJAUT**

- Exibe as autoridades dos Usuarios aos objetos
- Permite a inclusão e modificação de autoridades
- Interativo

- **GRTOBJAUT**

- Concede autoridade a objetos
- Interativo
- Batch

- **RVKOBJAUT**

- Retira/anula autoridade a objetos

- **DSPOBJAUT**

- Exibe a autoridade para objetos





# Listas de Autorização

- Contém uma Lista de usuários com suas respectivas autoridades sobre os objetos
- Permite que todos os usuários da lista tenham autoridades diferentes para um objeto
- É especificada no momento da criação do objeto
- Autoridade específica sobrepõe a lista de autorização
- É um objeto por si só



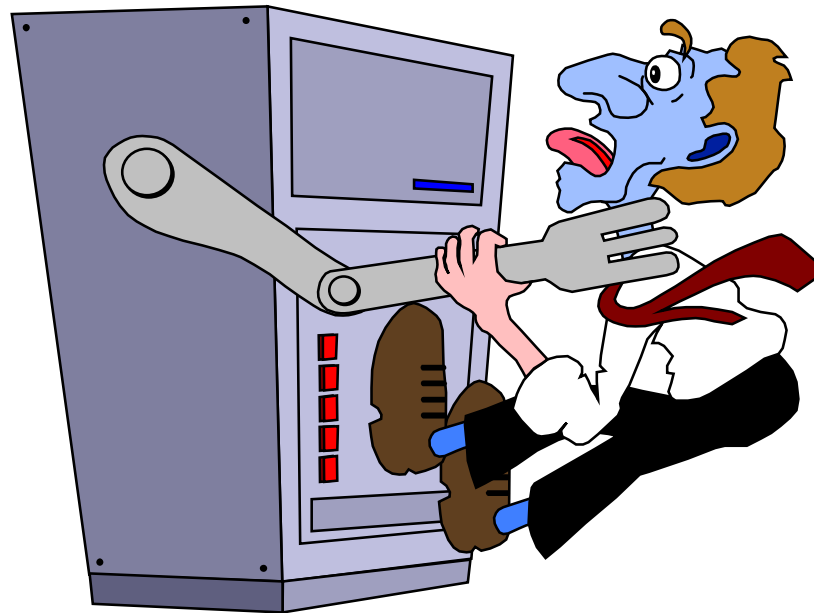




# Group Profiles

- Dá a mesma autoridade aos objetos para um Grupo de Usuários
- Quando um elemento do grupo cria um objeto, este pode pertencer ao Usuário ou ao Grupo
- Facilita o trabalho de atribuição de autoridades a todos os elementos do Grupo
- É criada através do comando CRTUSRPRF (\*NONE)
- Autoridade Específica sobrepõe a autoridade de Grupo





# Laboratórios

