# SAP

## P_SECAUTH_21 Exam

### Certified Technology Professional - System Security Architect

### Questions & Answers
### Demo

# Version: 4.0

## Question: 1

User1 grants role 1 to user2. Who can revoke role 1 role from user2?

A. The system OBA user
B. The owner of role 1
C. Only User1
D. Any user with the 'ROLE ADMIN' database role

**Answer: D**

Explanation:

## Question: 2

Why should you create multiple dispatchers in SAP Identity Management? Note: There are 2 correct answers to this question.

A. To accommodate scalability
B. To support fail-over scenarios
C. To handle password provisioning
D. To handle special network access requirements

**Answer: A, D**

Explanation:

## Question: 3

What is required when you configure the PFCG role for an end-user on the front-end server? Note: There are 2 correct answers to this question.

A. The catalog assignment for the start authorization
B. The S_RFC authorization object for the OData access
C. The Fiori Launchpad designer assignment
D. The group assignment to display it in the Fiori Launchpad

**Answer: A, D**

Explanation:

## Question: 4

In your system, you have a program which calls transaction
A. Users with access to this program can still execute transaction A without explicit authorizations given to this transaction. How do you prevent the access of users to the transaction A from within the program?
A. Make sure you do NOT assign transact on A to the authorization object S_TCODE in the role that you assign to the unauthorized users.
B. Maintain SE93 with authorization objects for transact on A.
C. Maintain the check indicator in table TCDCOUPLES
D. Ensure that transact on A is NOT assigned into the same program authorization group

**Answer: B**

Explanation:

## Question: 5

The SSO authentication using X.509 client certificates is configured. Users complain that they can't log in to the back-end system. The trace file shows the following error message: "HTTP request [2/5/9] Reject untrusted forwarded certificate". What is missing in the configuration? Note: There are 2 correct answers to this question.

A. On the back-end, the profile parameter icm/HTTPS/verify client must NOT be set to 0
B. On the web-dispatcher, the SAPSSLS.pse must be signed by a trusted certification authority
C. On the web-dispatcher, the profile parameter icm/HTTPS/verify_client must be set to 0
D. The web dispatcher's SAPSSLC.PSE certificate must be added to the trusted reverse proxies list in icm/trusted_reverse_proxy_<xx>

**Answer: A, B**

Explanation: