ZaranTech

knowledge is Everything

GLOSSARY OF SAP SYSTEM SECURITY ARCHITECT

A Quick Reference Guide to SAP Terminologies

Get any SAP Video course -https://zarantech.teachable.com/courses/category/sap
Linkedin Learner Community page -https://www.linkedin.com/showcase/sap-learner-community/

Concept/Term	Definition
SAP Security	Refers to the protection of SAP systems from unauthorized access and data breaches. Involves roles, authorizations, encryption, and compliance.
Security Architecture	The structure of security measures within an SAP landscape. Covers network, application, identity, and data security layers.
Authorization Concept	A structured approach to granting users access to SAP functions. Based on roles, profiles, and authorization objects.
User Master Record	Stores user-specific information in SAP. Includes roles, parameters, and license type.
Authorization Object	Defines access control criteria for SAP transactions. Contains fields checked during access decisions.

Concept/Term	Definition
Role (PFCG Role)	A collection of authorizations assigned to users. Created and managed using transaction PFCG.
Profile Generator (PFCG)	SAP tool used to create roles, assign authorizations, and manage role menus. Central to user access management.
SU01	Transaction to create and maintain SAP users. Allows updating roles, profiles, parameters, and logon data.
SUIM	Reports and tools to audit and analyze authorizations. Helps in tracking role usage and user assignments.
S_USER_AUT	Authorization object that allows assignment of authorizations to users. Required by administrators.

Concept/Term	Definition
Composite Role	A role that groups multiple single roles. Assigned to users for ease of access management.
S_TCODE	Authorization object controlling access to transaction codes. Used to restrict direct T-code access.
SAP NetWeaver AS ABAP	The application server for ABAP-based SAP systems. Provides the core for user management and security.
Secure Network Communications (SNC)	Encrypts SAP GUI communication with the backend system. Ensures secure end-to-end communication.
SAProuter	A proxy that routes network traffic securely to SAP systems. Often used to control external access.

Concept/Term	Definition
SAP Web Dispatcher	Acts as a reverse proxy and load balancer. Routes HTTP(S) traffic securely in SAP landscapes.
SSL (Secure Socket Layer)	Encryption protocol for securing HTTP(S) communication. SAP supports SSL for web-based services.
Digital Certificate	A cryptographic key pair used to identify systems or users. Used for secure authentication and encryption.
SAML 2.0	Single sign-on protocol used for browser-based authentication. Enables federated identity management.
SAP Identity Management (IDM)	Central solution for managing user identities and provisioning across systems. Supports workflows and compliance.

Concept/Term	Definition
SAP GRC (Governance, Risk, and Compliance)	Suite of tools to manage risk, enforce SoD policies, and handle access requests. Integrated with SAP Security.
SoD (Segregation of Duties)	Principle to avoid conflicts by separating critical duties across users. Prevents fraud and misuse.
S_BCE_68001410	Authorization object to allow table access via SE16/SE11. Must be restricted to prevent data leaks.
Security Audit Log (SAL)	Logs critical activities such as logins, RFC calls, and failed access attempts. Helps in forensic analysis.
System Log (SM21)	Captures technical events like errors, restarts, or unauthorized access. Useful in root cause analysis.

Concept/Term	Definition
Change Document Log	Tracks changes made to user and role data. Enables audit trails for critical updates.
S_RFC	Authorization object for RFC access to SAP functions. Used to secure system-to-system communication.
RFC (Remote Function Call)	Protocol used to call functions in other SAP systems. Needs strict control to prevent misuse.
Authorization Trace (ST01)	Used to trace missing or failed authorization checks. Helps identify required objects.
Security Optimization Service (SOS)	SAP-delivered service that evaluates the security posture of a system. Provides recommendations.

Concept/Term	Definition
SAP EarlyWatch Alert	Automated monitoring service that includes performance and security recommendations. Generated weekly.
SAP Solution Manager	Central tool for monitoring, maintenance, and compliance reporting in SAP landscapes.
User Buffer	Cached authorizations stored at user logon. Refreshed only at re-login or manual reset.
User Types	Defines purpose and access level of users (Dialog, System, Communication, etc.). Important for license and security.
S_USER_GRP	Controls user group assignment and administration. Useful for team-based access control.

Concept/Term	Definition
S_TABU_DIS	Governs access to table maintenance using authorization groups. Secures direct table updates.
S_PROGRAM	Controls execution of report programs. Restricts access to specific ABAP programs.
Critical Authorizations	High-risk access rights that must be reviewed periodically. Includes table access, debugging, and user admin.
Security Notes	SAP publishes these to fix security vulnerabilities. Regular implementation is critical for compliance.
Patch Management	Process of applying SAP Notes and kernel patches. Ensures systems are secure and up-to-date.

Concept/Term	Definition
Transaction Logging	Tracks execution of T-codes for audit purposes. Helps identify unauthorized or unusual behavior.
Encryption Key Management	Handles the lifecycle of keys for encryption. Important for securing HANA, SSL, and file-level security.
SAP Data Privacy Tools	Includes data masking, pseudonymization, and logging. Supports GDPR and data protection compliance.
Enterprise Threat Detection (ETD)	SAP's real-time monitoring solution for detecting cyber threats. Integrates with SIEM systems.
Security Baseline Template	SAP's checklist for securing different components. Covers ABAP, HANA, OS, and DB layers.

Concept/Term	Definition
User Comparison	Aligns user master records with current role definitions. Ensures consistent access after role changes.
Audit Trail	Provides historical logs of access, changes, and errors. Vital for compliance and investigations.
Data Classification	Labels data based on sensitivity (Public, Confidential, Restricted). Used for access and encryption decisions.
SAP Fiori Security	Manages access to Fiori apps using OData services and roles. Includes UI-level and backend authorizations.
HANA User Roles	Role concept in HANA for SQL-based access control. Managed separately from ABAP roles.