Deloitte.

SAP

Towards Automated Certificate Management in Large SAP Environments

MAKING AN IMPACT THAT MATTERS since 1845

Executive Summary

The Organizations' SAP landscape is continuously growing to face market expectations which demands increasingly interactions between SAP Systems and Non-SAP Systems. Certificates are leveraged to authenticate and encrypt data during these interactions.

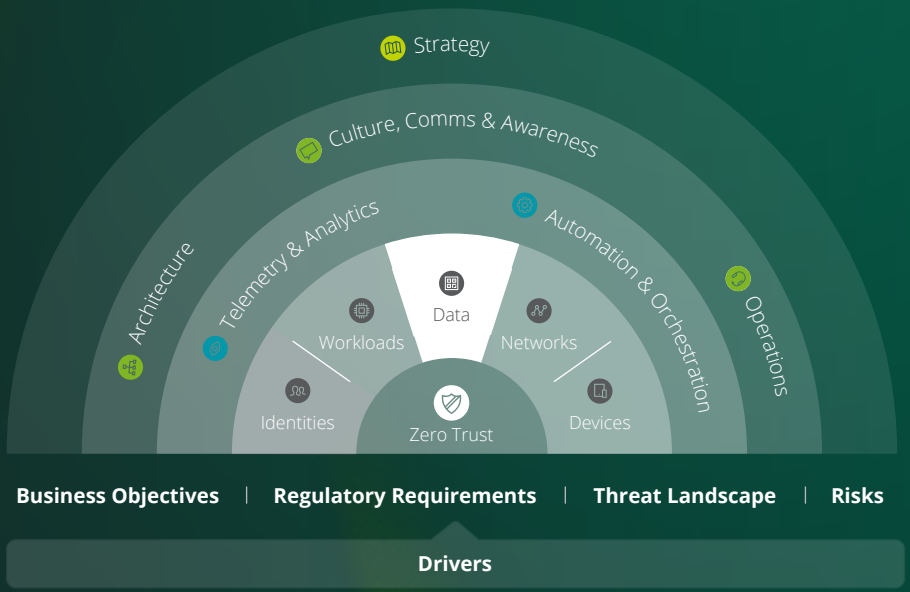
Zero Trust posture adopts the moto: "Never trust, always verify" and limits, as much as possible, the access to valuable information in the event of a cyber incident. By encrypting all existing communications, both inside out and outside in of SAP Systems, Zero Trust is being driven by ensuring information in transit is not disclosed, even if the malicious actor has access to network communications.

Manually managing certificates is no easy job. Added to the fact that in such large environments there are multiple connections to each one of the existing SAP systems, it makes the task almost not humanly possible. The renew failure consequence is devastating – if one certificate is not renewed in a timely manner the information's availability is not ensured and organizations may lose revenue. As certificate management is a repeated effort, there is a huge potential of automation which is itself a Zero Trust driver.

Executive Summary

Following the series of stories launched by the "Towards a Zero Trust Architecture in SAP Landscape"[1] paper, this story presents a possible approach to automate the certificate management process. Specifically, expose the struggle when manually managing certificates and present a High-Level solution to address this adversity, including connections from an SAP System to both SAP and Non-SAP Systems.

This story is focused on the **Data domain** of the Deloitte's Multidisciplinary Zero Trust Framework[2]:



STRATEGY LAYER
Zero Trust strategy should be aligned to the business drivers in a way that the journey is supporting the business, ensuring organization-wide adoption, future readiness and agility

GOVERNANCE LAYER
Zero Trust governance ensures a cohesive top-down strategy that considers stakeholders consensus to achieve necessary cultural, architectural and operational changes

ENABLING LAYER
Enabling layers help automate & orchestrate enforcement policies while continually analyzing enforcement decisions to identify Zero Trust violations

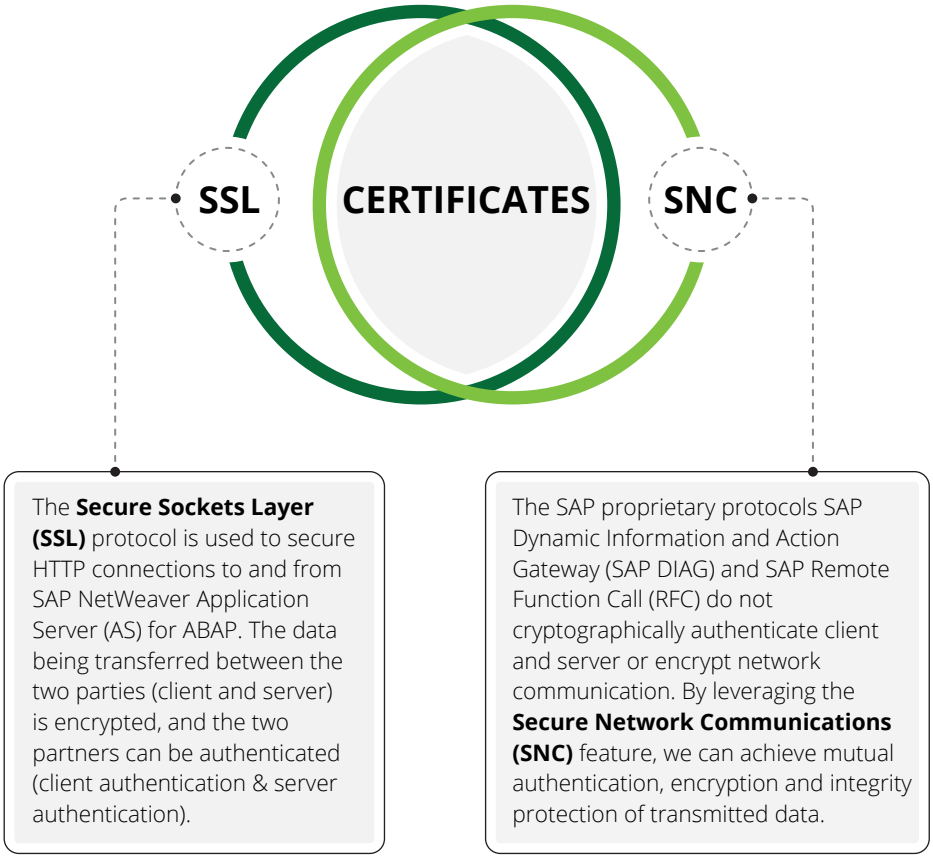
CORE DOMAINS
Zero Trust model is built upon strong foundational capabilities across five foundamental domains. The maturity across these domais will utimately determine Zero Trust maturity

[1] Link
[2] Link artigo

Secure connections in the SAP Environment

Protocols and Certificates

The Data Domain in the Deloitte's Multidisciplinary Zero Trust Framework ensures data in all states (e.g.: in-motion, at rest, in-change, in-use) and throughout the data lifecycle is protected, visible and under control. In SAP, there are mainly two protocols that can be leveraged to implement the in-motion protection on top of the existing SAP connections. Both protocols come with the SAP Common Cryptographic Library and leverage **certificates** in their operating mechanism.



Certificates in SAP are stored in the Personal Security Environment (**PSE**), which is the storage location for the server's security information and contains:

- Private key
- Public key certificate of the server
- Certificates of trusted CAs

Each SAP System contains multiple PSEs which are used depending on the connection purpose:

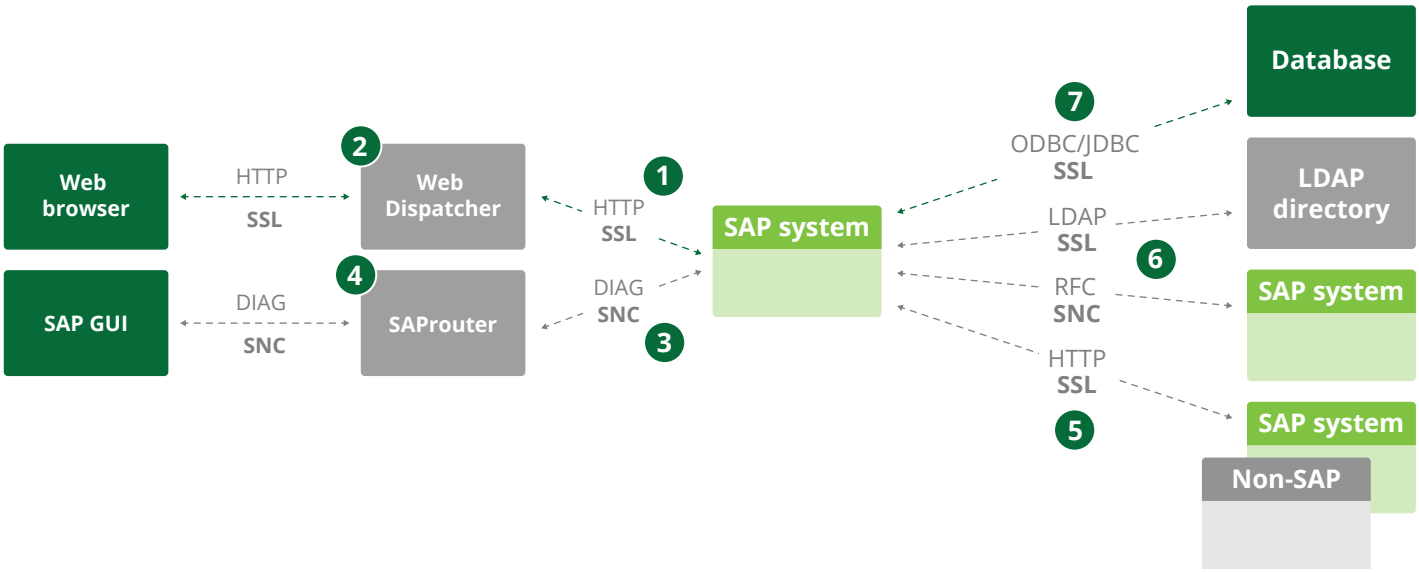
- System PSE: Digital Signatures
- SNC PSE: Used for SNC
- SSL server PSE: When the SAP system acts as the server component
- SSL client PSE: When the SAP system acts as the client component

Secure connections in the SAP Environment

Secure SAP Connections

Typically, the SAP Environment establishes a complex architecture that comprises a massive set of connections to fulfill a large variety of services. Therefore, multiple connection types are deployed to allow the communication between SAP Systems and SAP/Non-SAP Systems.

Follows a diagram representing the potential connection types that may exist in a large SAP environment along with the used protocol as well as the secure mechanism that can be deployed.



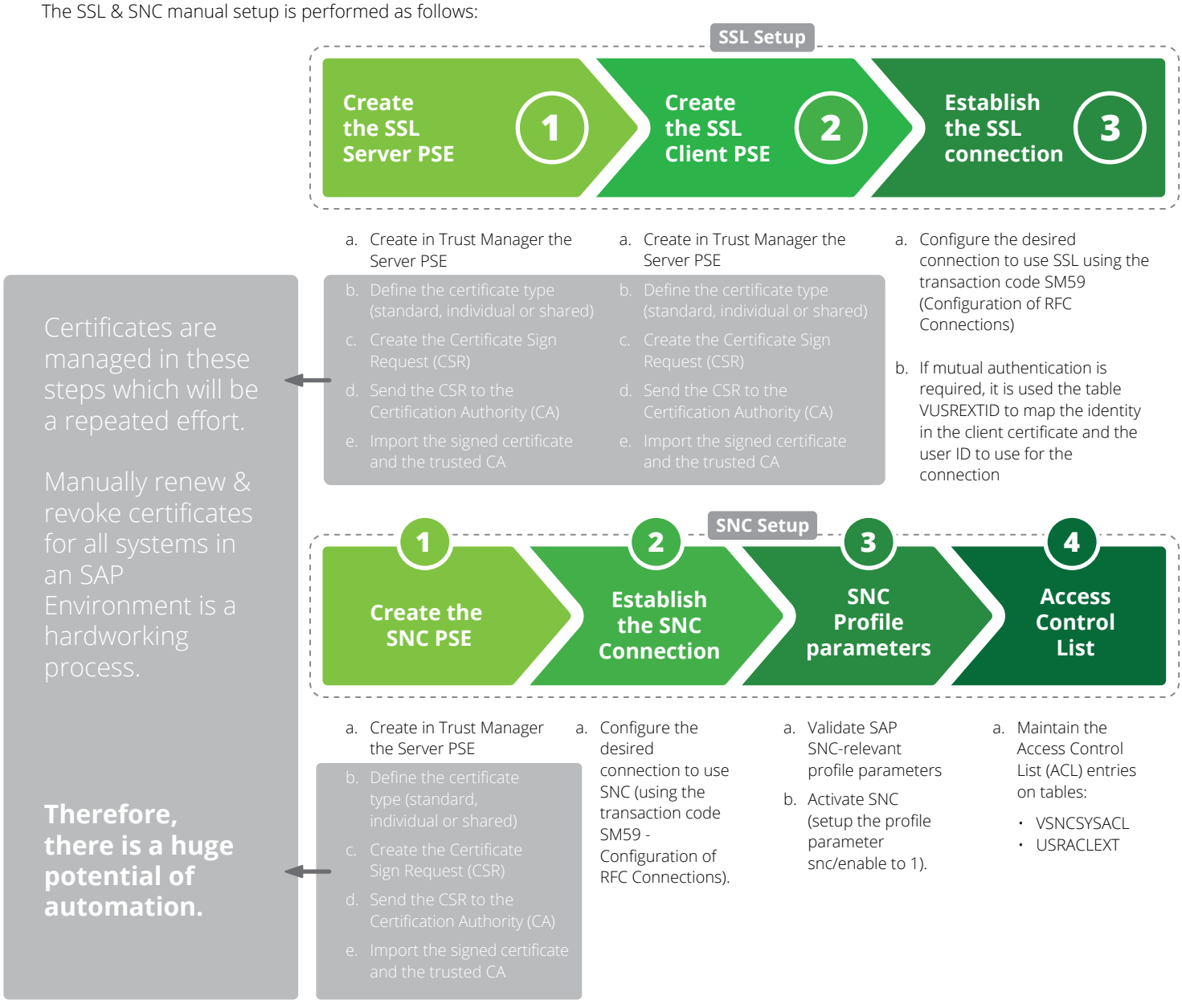
N	Source	Destination	Connection Type	Secure Protocol
1	SAP System	Web Dispatcher	HTTP	SSL
2	Web Dispatcher	Web Browser	HTTP	SSL
3	SAP System	SAPRouter	DIAG/RFC	SNC
4	SAPRouter/ SAP AS	SAP GUI/ WEB GUI	DIAG/RFC	SNC
5	SAP System	SAP System/ Non-SAP System	HTTP	SSL
6	SAP System	SAP System	DIAG/RFC	SNC
7	SAP System	Database (e.g.: HANA)	ODBC/JDBC	SSL

Certificate Management

Manual Certificate Management

As discussed, SSL & SNC secure protocols leverages certificates to secure SAP Communications. To use these protocols, a set of steps need to be followed to ensure the correct configuration for each existing connection.

The SSL & SNC manual setup is performed as follows:

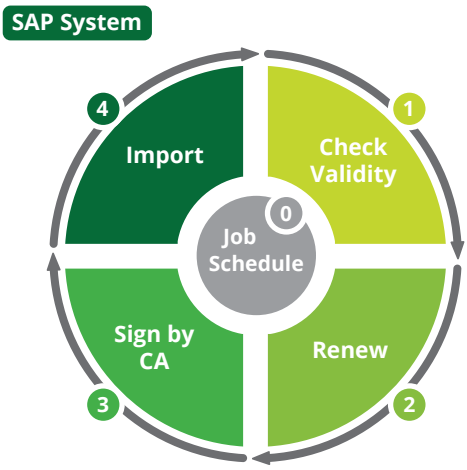


Certificate Management

Automated Certificate Management

To reduce company's human resources effort and tackle the possible human failures, each SAP system should be able to automatically create a certificate, send it to be signed by the CA and import the response back into the system.

Programmatically, this can be performed as follows:



0. A job schedule should be developed that runs at a predefined time.
1. The certificates' validity of all System's PSEs should be checked and the renew process begins if the certificate ends the validity before a predefined number of days.
2. A new certificate is created by the system.
3. The certificate is forwarded to the CA, signed and returned to the system.
4. The certificate signed by the CA is imported into the respective PSE.

Depending on the system type, different approaches may be defined. For AS ABAP & JAVA Systems, a standard SAP report can be used while custom developed scripts should be deployed for other systems. Either way, **Secure Login Server** is a critical component when automating this tough activity.

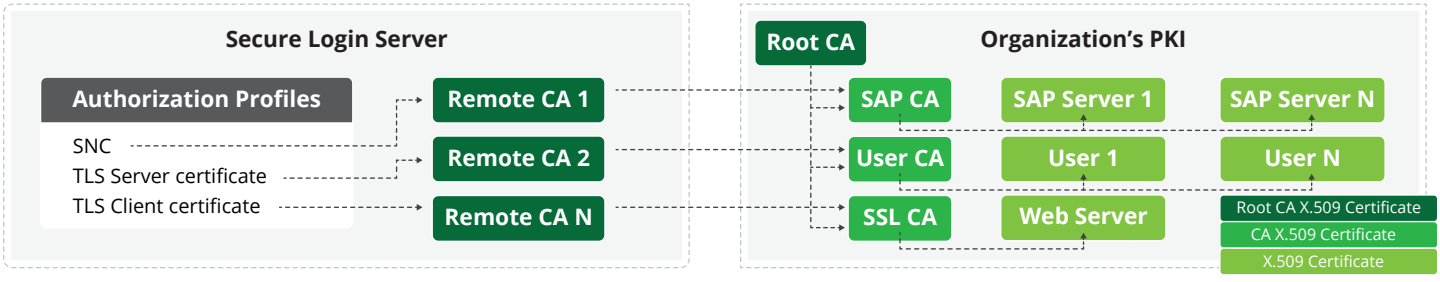
Follows the Secure Login Server role in automation as well as different approaches considering the connection types.

Secure Login Server Role in Automation

The **Secure Login Server** (SLS) is deployed in an AS Java and provides standard X.509 certificates for end users (short term) and application servers (long term). Although the SLS delivers an out-of-the-box PKI infrastructure, it is possible to integrate with an existing PKI.

Specific configurations must be followed for a successful automated certificate management implementation. Specifically, remote CAs should be defined and configured to point to the organization's CAs and authorization profiles should be created leveraging the remote CAs defined.

The authorization profiles are used by the SAP System during the certificate renewal process.

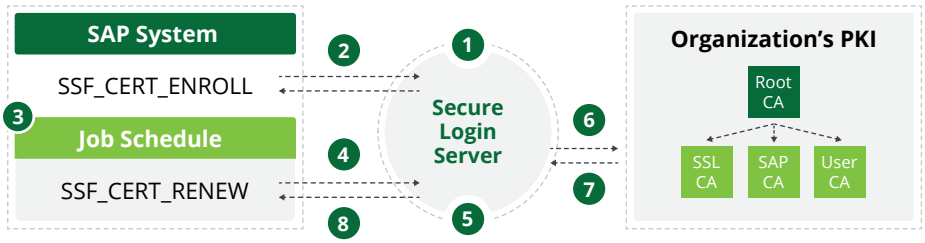


Certificate Management

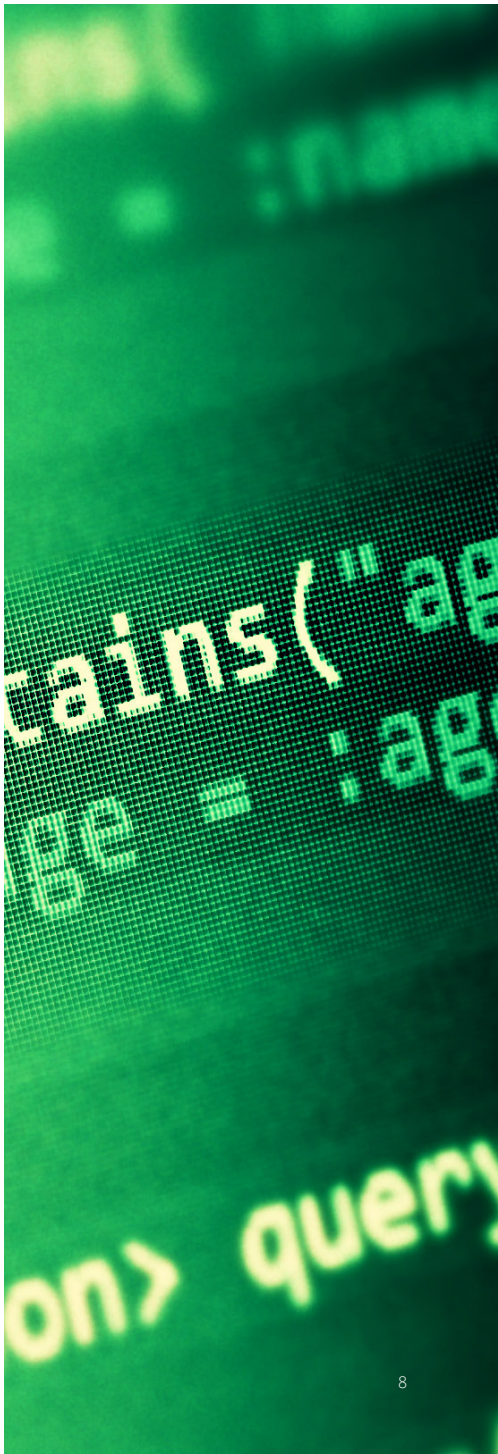
A. SAP AS ABAP & JAVA: High-Level Architecture

SAP Report SSF_CERT_RENEW can be leveraged for certificate renewal of both ABAP and Java Application Servers. This report enables the integration with SLS and enables the usage of the configured authorization profiles.

After the configuration and enrollment process is completed, the certificate renewal process can be executed at regular intervals. The following approach may be implemented:



1. Secure Login Server Configuration (including the Logon Stack, the Registration Agent Profile, the Application Server Profiles and the Application Server Profile Group).
2. Enrollment of SAP System by executing the SSF_CERT_ENROLL report. This report enrolls the SAP System with the SLS and creates a PSE (SSL Client Certificate SAPSLS) in the SAP System that contains the certificate that will be further used during the renewal process.
3. Create a job schedule (in transaction SM37) to run at a predefined time. This job checks the validity of the certificate and identifies whether is about to expire.
4. For a certificate about to expire, execute SSF_CERT_RENEW report defining the PSE target to renew and the respective SLS Authorization Profile.
5. The adequate Authorization Profile is executed and the defined remote CA (that points to the Organization's PKI) is leveraged.
6. The certificate is sent to Organization's CA to be signed.
7. The signed certificate is retrieved to SLS.
8. The SLS forwards the signed certificate to the SAP System where it is imported to the respective PSE.



Certificate Management

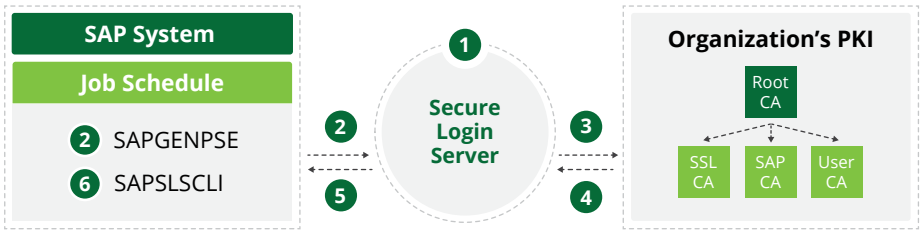
B. Other SAP Systems: High-Level Architecture

Certificates for other systems like HANA or Web Dispatcher, should also be renewed automatically. As SSF_CERT_RENEW report cannot be used, a different approach should be defined. There are two tools that can help with this activity:

• The **sapslscli** is a command line tool delivered with SAP Single Sign-On 3.0 that can be leveraged in such way to manage the certificate lifecycle using operating system resources.

• The **sapgenpse** is a command line tool that enables the PSE creation and management.

Following the same SLS configuration as in Approach A, the next high-level architecture can be deployed:



1. Secure Login Server Configuration (including the Logon Stack, the Registration Agent Profile, the Application Server Profiles and the Application Server Profile Group).
2. A job schedule (cron jobs or windows batch scheduler) should be created including the following command lines to fulfill the required activities, as follows:
   a. *"sapgenpse get_my_name"*: Check the validity of the certificate and identify if is about to expire.
   b. *"sapslscli enroll"*: Execute the certificate renewal and leverage the Authorization Profile previously configured.
   c. *"sapslscli renew"*: Execute the certificate renewal and leverage the Authorization Profile previously configured.

   The following steps are performed automatically:
3. The certificate is sent to Organization's CA to be signed.
4. The signed certificate is retrieved to SLS.
5. The certificate is installed in the SAP Server.
6. The validation of the renewal process may be included in the scheduled job by levering the *"sapgenpse get_my_name"*.

Future Challenges

This story focused on automating the certificate management process leaving out several certificate-related topics that we consider relevant to highlight.

Certificate Revocation

It may be necessary to blacklist a certificate due to specific reason (e.g.: certificate exposure, server decommissioning).

The revoked certificate should be included into the CA Certificate Revocation List (CRL) to tackle the potential risk of certificate usage for malicious activities.

When facing this situation, a pre-defined process should already be in place so it can be followed in a timely manner.

HINT

SAPGENPSE tool is recommended by SAP to manage the CRL, by leveraging the "get_crl" command.

Certificate Authority Certificate Renewal

Is a generic cybersecurity best practice to renew the certificate authority certificate - the strategy implemented in the organization dictates the periodicity.

An automated CA certificate renewal process should also be defined and deployed. In addition, when the CA certificate is renewed, all systems supported by certificates signed by that CA will require attention. In fact, all these systems should follow the renew process considering the new CA.

A process to handle this activity should be thought in advance so that minimal disruption of services is ensured.

HINT

Enable the trust certificate list feature in SLS to automize the CA List update in the SAP Server.

Monitoring

Having a global overview regarding the certificates management process is must-have in a large organization. This feature will simplify the metric extraction as well as detection in a timely manner in case of certificate renewal issues.

Currently, SAP does not provide an out-of-the-box solution to monitor the automated certificate renew process discussed in this story. For this matter, a solution should be custom developed.

HINT

Avantra is a solution that can help in this topic – leverage the SSLCertificatesValidity to verify the certificate validity of ABAP systems and build dashboards to track this activity!

Authors

Andre Correia Sousa
Portugal SAP Security Expert
andrsousa@deloitte.pt
+351 962753775

Matthias Sill
Germany SAP Security Expert
msill@deloitte.de
+49 15158000306

Contacts

Andre Correia Sousa
Portugal SAP Security Expert
andrsousa@deloitte.pt
+351 962753775

Antony Jose Vallookaran
Poland SAP Security Expert
anvallookaran@deloittece.com
+48 123944429

Fabio Bonanni
Italy SAP Security Expert
fbonanni@deloitte.it
+39 0283326347

Gabriele Piersanti
Spain SAP Security Expert
gpiersanti@deloitte.es
+34 638315587

Hans Peersman
Netherlands SAP Security Expert
hpeersman@deloitte.nl
+31 882887368

Marc Noergaard
Denmark SAP Security Expert
mnoergaard@deloitte.dk
+45 22300140

Marisa Geldenhuys
UK SAP Security Expert
mgeldenhuys@deloitte.co.uk
+44 7552 549146

Matthias Sill
Germany SAP Security Expert
msill@deloitte.de
+49 15158000306

Rajwinder Singh
USI SAP Security Expert
rajwindsingh@deloitte.com
+1 (470) 3624637

Vaibhav Jani
Canada SAP Security Expert
vaijani@deloitte.ca
+1 4167757269

Vikas Bhan
Belgium SAP Security Expert
vbhan@deloitte.be
+ 32 24558752

Deloitte.