



How to Secure Privacy Data in a SAP S/4HANA Hybrid Landscape

Paul Young, Delivery Manager, Southern California Edison
Tong Zheng, Security Expert, SAP America
Session ID # 84339

About the Speakers

Paul Young

- Delivery Manager
Southern California Edison
- 20 years in SAP Solution
Architecture, 16 years in the
Utility industry

Tong Zheng

- Security Expert, SAP
America
- 15 years with SAP Service &
Support. Focus on
Cybersecurity and
Compliance

Key Outcomes/Objectives

1. Data Privacy in cybersecurity
2. SAP S/4HANA security features
3. Data Encryption at rest and in transit
4. Masking and logging

Agenda

- Introduction: Data Privacy in Cybersecurity – 5 min
- SAP S/4HANA Security Features – 20 min
- Masking and Logging – 10 min
- Q & A – 5 min

Introduction

- Digital innovations and transformations are re-shaping everyone's life. Technologies such as in-memory computing, cloud, and mobility have made an impact on enterprises.
- Companies that embrace the digital transformation are facing increased Cyber threats and attacks. Security breaches can impact organizations and their customers.
- One of the first line of defense measures is to protect companies' confidential data and business partners' privacy. And the first and foremost defense is to encrypt data wherever feasible.

In this session, you will be presented the information protection features available in a SAP S/4HANA and C/4HANA hybrid system.

SAP S/4HANA Security Framework Overview

➤ **User Management & Authentication**

- User and identity management
- GRC and IDM integration
- Single sign-on (Kerberos, SAML, ...)

➤ **Authorization**

- Role management framework
- Row-level access control (Analytics)
- LDAP integration (HDB)
- Integrated application authorizations (XAS)

SAP S/4HANA Security Framework Overview

➤ Encryption

- At rest and in transit
- Backup encryption
- Application encryption
- Column encryption

➤ Data Masking

- SQL data masking
- UI Masking and logging
- Custom masking

SAP S/4HANA Security Framework Overview

➤ **Anonymization**

- Real-time data anonymization
- Custom definition of anonymization views
- Fully integrated with authorization framework

➤ **Auditing**

- Security logging for all system events
- Customizable policies
- Log read and write access to critical data

SAP HANA Encryption Features

Comprehensive encryption



Communication encryption

Encrypt data in transit using TLS/SSL



Backup encryption

Encrypt backups with SAP HANA native functionality (HANA2) or 3rd party backup tools



Data at rest encryption

Encrypt data stored on disk using data volume encryption and log encryption (HANA2)



Column encryption

Encryption of individual table columns with HANA client-controlled keys (HANA2)



Application encryption

Encrypt security-relevant application data (application encryption API)

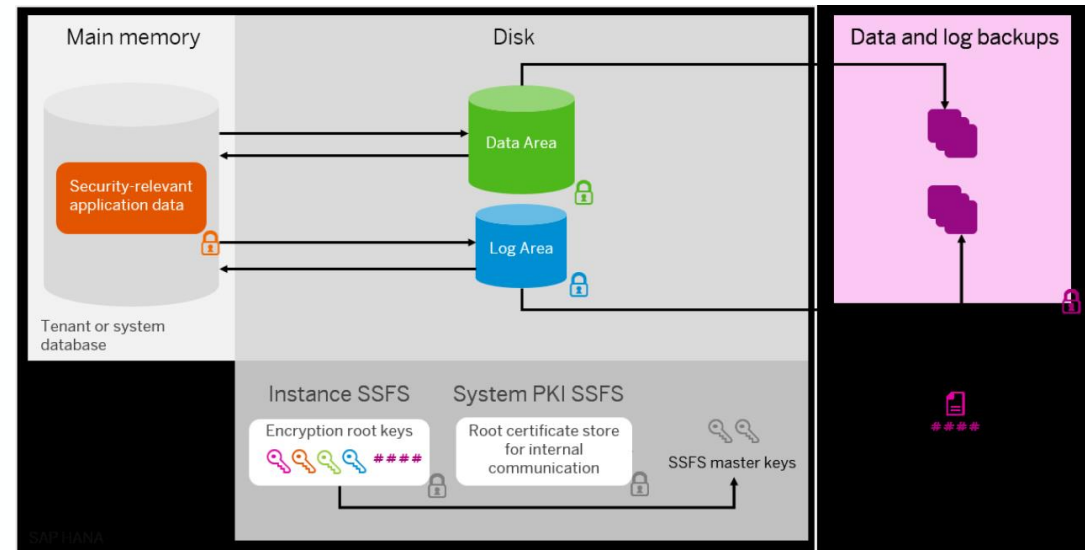
Source: SAP

SAP HANA Encryption Data at Rest

Data-at-Rest Encryption

To protect data saved to disk from unauthorized access at the operating system level, the SAP HANA database supports data encryption in the persistence layer for the following types of data:

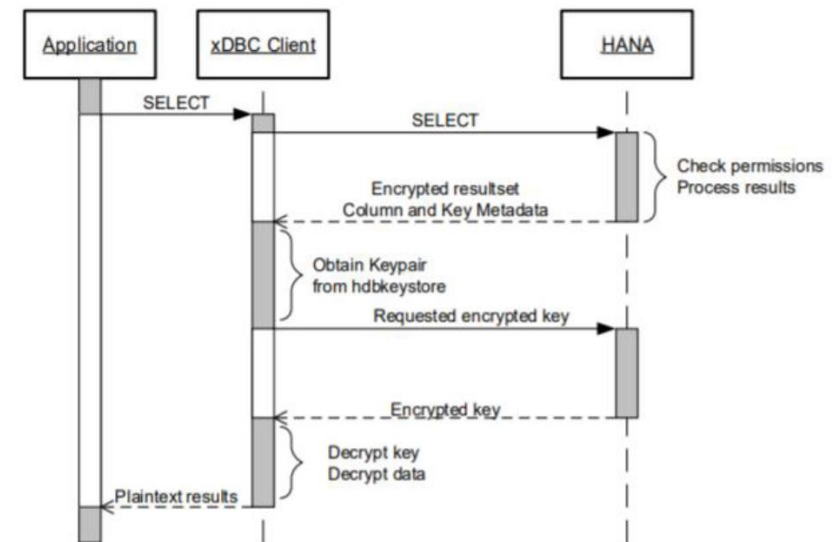
- Data in data volumes
- Redo logs in log volumes
- DB backup encryption



Source: SAP

SAP HANA Client Side Encryption

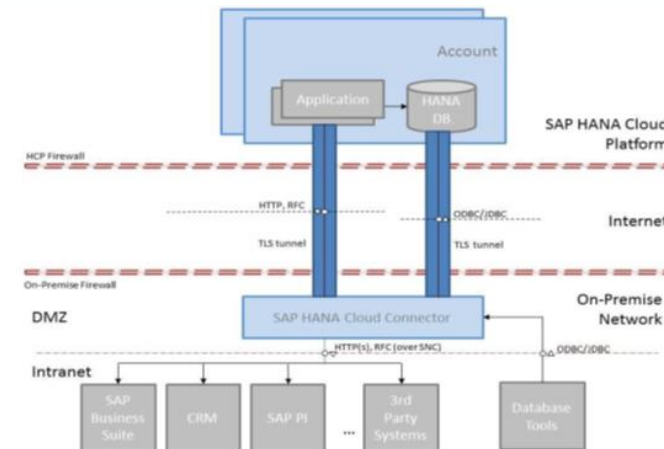
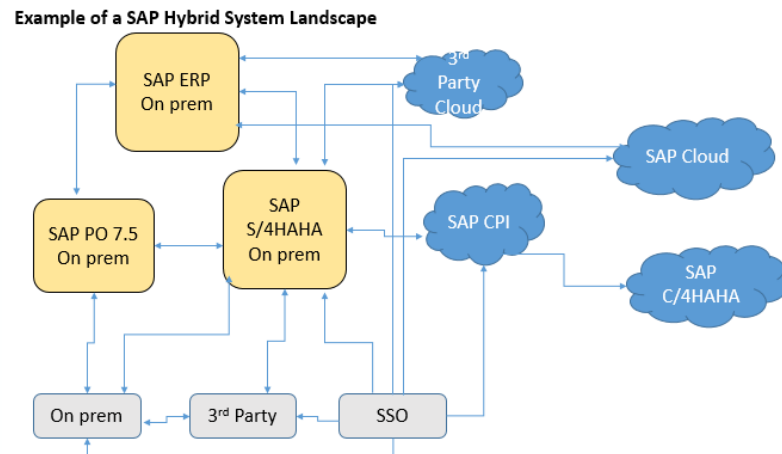
- With client-side data encryption (HANA 2.0 sp3), columns that contain sensitive data can be encrypted by using an encryption key accessible only by the client.
- Column data is encrypted and decrypted on the client-driver, allowing the application to read and write data in clear text form.
- As a result, client-side encryption provides a separation between those who own the data (the users) and those who manage the data (e.g. DBA).
- Sensitive column data is encrypted with a symmetric column encryption key that is encrypted using a client key pair.
- To access the encrypted data, an application must use a **client driver** that supports client-side encryption (currently only xDBC are supported), and the client must have access to the CEK that encrypts the column.



Source: SAP

Hybrid Secure Communication

- SAP relies on encryption technology that uses HTTPS and secure RFC to prevent unauthorized parties from intercepting network traffic.
- The encryption is based on the Transport Layer Security (TLS) protocol.
- For HTTPS, *system certificate* can be configured in the Cloud Connector which is used for the trust relationship between the Cloud Connector and the connected on premise systems.
- The Cloud Connector also supports principal propagation of the cloud user identity to connected on premise systems.
- Exchange the self-signed X.509 certificate of the Cloud Connector administration UI by a certificate that is trusted by your company and the company's approved Web browser settings.



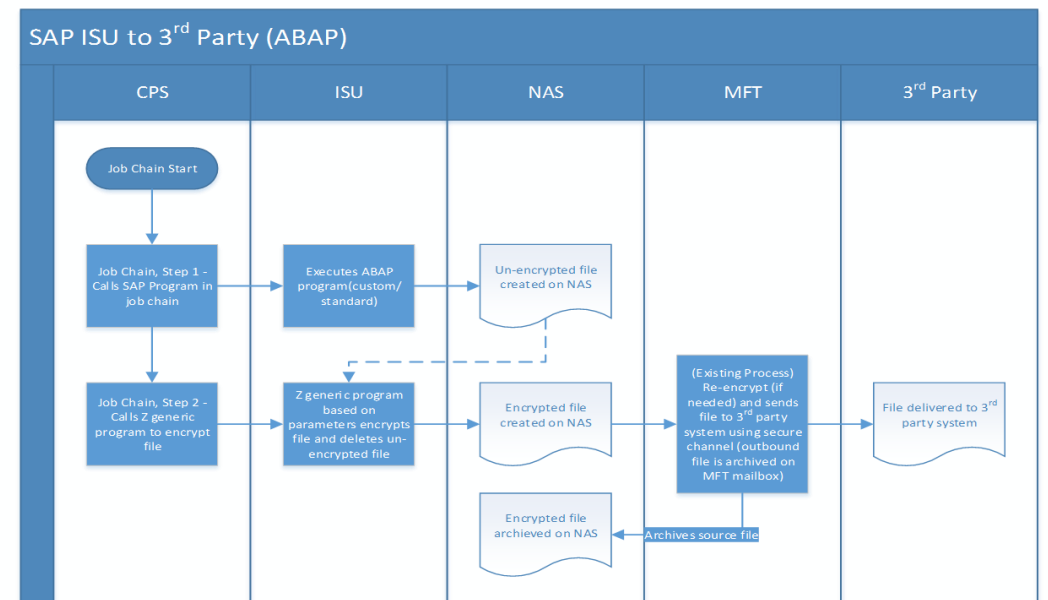
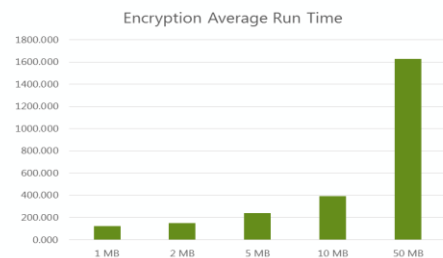
Source: SAP

File Encryption

- SAP interfaces with 3rd party and legacy systems use file transport protocols, file share, and are encrypted with certificates
- SAP CPS file watcher is running to encrypt files upon writing to the file system with PKI
- Files can be decrypted with a custom function module
- Optionally, the entire disk can be encrypted

File Based Data Encryption Solution Overview (cont'd)
POC Encryption Run Times (millisecond)

Runs	1 MB	2 MB	5 MB	10 MB	50 MB	
Run 1	123.904	150.317	233.084	388.211	1613.857	
Run 2	143.640	138.528	261.308	390.056	1625.531	
Run 3	111.403	174.682	231.749	385.514	1659.350	
Run 4	130.542	139.408	230.329	411.629	1629.563	
Run 5	109.450	153.429	233.729	382.845	1618.674	
Average	123.788	151.273	238.040	391.651	1629.395	



SAP HANA Data Masking

- Additional controls on tables and views of native HANA applications
- Not compatible with ABAP stack on HANA
- Not possible to mask encrypted columns
- Protects sensitive data in particular columns
- Specified directly in the definition using CREATE TABLE/VIEW statement
- Access will return masked data
- Access is controlled by the object privilege UNMASKED

		SELECT privilege	
		Not granted	Granted
UNMASKED privilege	Not granted	Not authorized	###-##-####
	Granted	Not authorized	123-33-1123

Source: SAP

SAP UI Masking

What is UI Masking?

- Sensitive data are masked on the server side and editing is blocked in SAP user interfaces; resulting in consistent protection also in table display, value help, export, download, print etc.
- Provides unmasked data to specifically authorized users/roles only –on top of existing authorization system (PFCG)
- Small-scale, auditable, achievable “access trace” in case of access to protected data fields

How does it work?

- Extensive configuration options on field level:
- Which fields are masked in which way – including mass configuration report for a quick start.
- Which users/roles are shown clear data
- Which accesses are traced
- Complex business logic (e.g. attribute based masking, based on SAP-internal attributes) can be implemented via BADI
- Highly performant –minimal system requirements

SAP UI Masking – cont'd

Configuration: two simple steps...

1. Define fields to be masked, and rules

- Define which fields are masked.
- Configure on field level how a field is displayed. Define on digit base whether and how data are masked.

2. Register authorized users per field

- In transaction PFCG, assign users to the UI Masking authorization a role.
- Users assigned to these roles will be able to see unmasked values for the applicable fields
- BADIs available to introduce customized business logic determining who has access

SAP UI Masking – cont'd

UI Masking: Benefits for Regulatory Compliance

Benefits: **Data Anonymization & Data Minimization**

Decrease the risk of leaking sensitive data

- Hide information “not required for the job” (principle of data minimization)
- Hide (sensitive) personal information
- Consistent protection, also for download and printouts

Anonymize information – allowing to further processing (test scenarios, data export)

Alternative to data “blocking”

- Cost effective alternative to ILM-based “Blocking”
- Keeps reports/aggregates accurate

Support requirements relating to “privacy by default” and “privacy by design”

SAP UI Masking – cont'd

UI Logging: Benefits for Regulatory Compliance

Benefits: **Data Access Transparency and Reduction of Data Access**

Compliance mandate: where you need to keep (personal) data accessible, you need to log access to be able to comply with notification duties in case of a breach – and quickly (“72 hours”)

- Ability to decide on and provide a breach notification in time (72h) and in quality (concerned data objects, and afflicted persons)
- Ability to identify (and stop) the person(s) responsible for a data leak
- effective co-operation with authorities in case of review

SAP UI Masking – cont'd

UI Logging: Benefits for Regulatory Compliance



Key element to successful logging: not only creating, but being able to leverage a log to identify unauthorized, non-compliant or malicious activity

- automated controls to be warned in case of dubious data access
- manual controls to review the logs periodically and in-depth

Builds a psychological barrier against non-task related data access

- decreases the probability and magnitude of data leaks
- soft factor “data minimization”

Coverage: **10 “channels”**

UI technology	UI Masking 	UI Logging 
SAP GUI for Windows / HTML / Java	✓	✓
WebDynpro ABAP	✓	✓
CRM Web Client UI	✓	✓
RFC/BAPI and Web Services	project based	✓
BW Access (BEx Web/Analyser, BW-IP, BICS, MDX)	project based	✓
UI5/Fiori	✓	✓

Source: SAP

SAP UI Masking – cont'd

Options:

1. Custom Utility Class

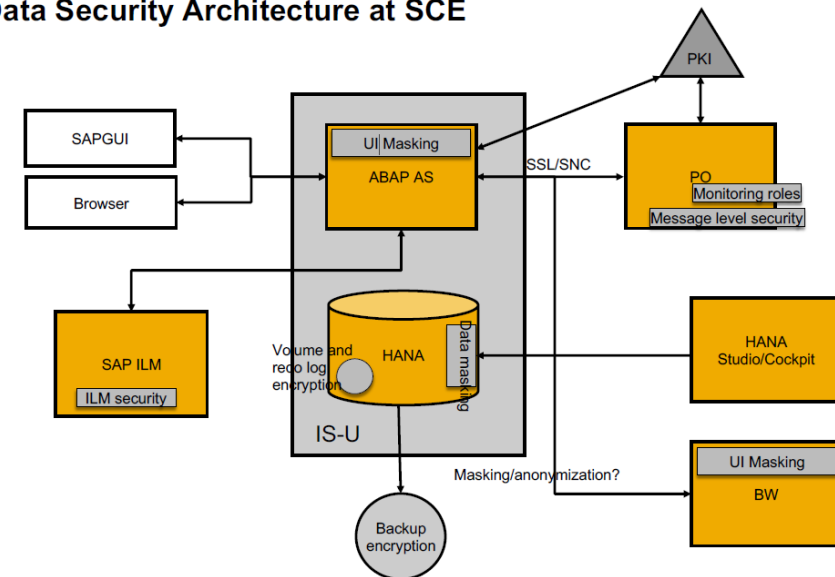
This enhancement will require the creation of a custom utility class that will mask and unmask the sensitive information using these function modules:

- BAPI_IDENTIFICATIONDETAILS_GET
- BAPI_BUPA_BANKDETAILS_GET
- BUP_BANK_GET
- BUP_BANK_GET_ALL
- BUP_BUPA_PBO_MISC
- BUP_BUPA_PAI_MISC
- BUS_CHANGE_DOCUMENT

2. Custom T-code/Screen Variants

- Customizing standard t-codes by defining screen variants
- Field status group to suppress fields in t-codes
- Create custom authorizations objects to secure screen/fields
- Hide the sensitive fields in screens
- Each t-code has to be done manually
- User exists can also be used in standard t-codes

End to End Data Security Architecture at SCE



More Information

Documentation [SAP Help Portal](#):

- Security Guide, Administration Guide, Developer Guide, SQL Reference Guide

Secure configuration guidelines

- [SAP HANA Security Checklists and Recommendations](#) are provided to accompany the detailed Security Guide
- [SAP Security Baseline Template](#)
- [DSAG Prüfleitfaden ERP 6.0](#) (by the German SAP user group)

Whitepaper

- [SAP HANA Security Whitepaper](#)

Best practices

- [Best practices and recommendations for developing HDI-based roles](#)

Training

- [HA 240](#)

SAP Notes (login required)

- [2159014](#) FAQ: SAP HANA Security
- [1730928](#) Using external software in a HANA appliance
- [1730929](#) Using external tools in an SAP HANA appliance
- [1730930](#) Using antivirus software in an SAP HANA appliance
- [784391](#) SAP support terms and 3rd-party Linux kernel drivers
- [1730999](#) Configuration changes in HANA appliance
- [863362](#) Security checks with SAP EarlyWatch Alert
- [2021789](#), [2378962](#) SAP HANA revision and maintenance strategy

Key Points to Take Home

- Digital transformation is increasing security challenges
- Cloud applications bring additional complexity to security
- Security threats have been evolving and Cybersecurity is everyone's responsibility
- Regulations continue to increase both globally and domestically
- Establish your enterprise cybersecurity framework and control catalog
- SAP is a target for Cyber criminals and hacktivists, nation states, and internal bad actors
- Research and adopt industry leading security recommendations
- Select the secure, scalable, and quick and cost effective solutions

Take the Session Survey.

We want to hear from you! Be sure to complete the session evaluation on the SAPPHIRE NOW and ASUG Annual Conference mobile app.



Presentation Materials

Access the slides from 2019 ASUG Annual Conference here:

<http://info.asug.com/2019-ac-slides>

Q&A

For questions after this session, contact us at

paul.c.young@sce.com

tong.zheng@sap.com

Let's Be Social.

Stay connected. Share your SAP experiences anytime, anywhere.

Join the ASUG conversation on social media: **@ASUG365 #ASUG**

