

SAP Technology

CIO GUIDE

IT Security in Cloud and Mobile Environments

Table of Contents

3	Executive Summary
8	Introduction and Scope
12	Reference Concepts
23	SAP Products
29	Conclusion and Outlook
32	Find Out More
34	Glossary

The Authors

Andreas Schoknecht, Matthias Vogel, Anke Lilleike, and Nikica Josipovic are members of the Products & Innovation group at SAP AG.

Disclaimer

This document describes concepts that can help companies respond to security challenges. It contains current and intended strategies, developments, and/or functionalities of SAP® solutions, applications, and technologies and is not intended to be binding upon SAP to any particular course of business, product strategy, and/or development; its content is subject to change without notice.

This document is not subject to your license agreement or any other service or subscription agreement with SAP.

SAP assumes no responsibility for errors or omissions in this document. SAP does not warrant the accuracy or completeness of the information, text, graphics, links, or other items contained within this material. This document is provided without a warranty of any kind, either express or implied, including, but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or noninfringement.

SAP shall have no liability for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of these materials. This limitation shall not apply in cases of intent or gross negligence. The statutory liability for personal injury and defective products is not affected. SAP has no control over the information that you may access through the use of hot links contained in these materials and does not endorse your use of third-party Web pages nor provide any warranty whatsoever relating to third-party Web pages or their content.

All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, which speak only as of the publication date, and they should not be relied upon in making purchasing decisions.

1 Executive Summary

Companies today must operate efficiently within an intensively connected world. This means maintaining an infrastructure that may be on premise, in the cloud, or mobile and satisfying users who expect to access software from anywhere. IT security has become a key concern, with challenges like ensuring data privacy in the cloud, securing back-end access from mobile devices, and enabling single-sign-on (SSO) functionality in hybrid, on-premise, and cloud landscapes. Companies have to adapt policies, processes, people training, and architecture to overcome the IT security challenges in this extended world.

This guide discusses relevant IT security challenges, especially those driven by cloud and mobile trends, which can impact existing on-premise IT landscapes and lead to hybrid landscapes that combine on-premise and cloud solutions. As a leading application software vendor, SAP provides expertise on how to overcome these challenges and shares reference concepts and recommendations from the perspective of an application architecture.

1.1 STRUCTURE AND ROLE OF THIS GUIDE

In order to look at IT security challenges and related recommendations systematically, a common model for securing business information is used to provide a holistic view of business application security. As represented by this model, IT security is based on three elements:

- Securing information – addresses data privacy in the cloud and safeguarding information
- Securing interaction – addresses providing a secure on-premise landscape when it is integrated with cloud and mobile technologies
- Securing identities – addresses identity management and SSO in hybrid infrastructures

These three elements form the key pillars for establishing a secure business application architecture. The discussion of security challenges related to cloud and mobile trends focuses on these elements. To help you determine the relevance of each challenge for your business, each challenge is categorized. The appropriate IT responses and their benefits are explained in detail in "[Reference Concepts](#)." The document's conclusion includes a comprehensive list of resources for further information.

The IT responses provided in this guide are general and independent of any specific SAP® product. How SAP products can help meet these security requirements is detailed separately. For example, the popular bring-your-own-device (BYOD) trend is considered in light of how SAP software supports security for cloud and mobile technologies.



As a trusted advisor and reliable business partner to its customers, SAP takes security very seriously, leveraging standards and processes to build security into its software products from the very beginning.

This guide complements other SAP publications – security guides, product information, and security notes (see “Find Out More”). Whereas those publications provide security information written specifically for consultants and system administrators, this document is meant for IT management and enterprise architects. Its aim is to help verify and adapt existing security architecture strategies in an environment where the use of cloud and mobile technologies is prevalent.

Because it lists specific challenges, this guide can be used as a checklist when challenges within a company are examined. You will find recommendations on how to cope with those challenges, especially in the area of IT security.

1.2 CHALLENGES: CATEGORIES AND RELEVANCE FOR YOUR COMPANY

The challenges discussed here are categorized to help you determine the relevance of a specific challenge for your company. The categories are:

- Scenario – Not all challenges are relevant to all types of infrastructure. This guide uses three scenarios to categorize challenges:

- Cloud-only environment
- Hybrid environment comprising cloud-based and on-premise solutions
- Mobile environment, which may coexist with a cloud-only environment or hybrid environment
- Priority – Not all challenges are of the same urgency. Three levels of priority are recognized:
 - Very high: Challenges fundamental for all scenarios
 - High: Challenges faced by most companies that want an integrated solution today
 - Medium: Challenges based on the individual customer situation, environment, or business, with each reader deciding on the degree of relevance for his or her company based on details provided with the challenge
- Quality – The fitness of available solutions to address challenges varies. The following degrees are used to indicate their quality:
 - Mature: Stable and widely used
 - Enabled: Gaining traction
 - Evolving: Introducing emerging concepts that have been adopted by only a few innovative companies

Findings and recommendations are discussed based on this set of categories.



This guide considers IT security from three basic perspectives, which we consider the building blocks for establishing IT security: secure **i**nformation, secure **i**nteraction, and secure **i**dentities.

1.3 KEY FINDINGS

The following tables provide an overview of the challenges discussed in this paper. They are organized according to the three key pillars of IT security: achieving secure information, secure interaction, and secure identities. This categorization introduced above is indicated in the table as well to help you determine which challenges are most relevant for your company. The numbering tells you where to find the related details in “[Reference Concepts](#).”

1.3.1 Securing Information

In an interconnected world, information security must span diverse legal entities, even different countries, from cloud service providers to network providers to your own company. This leads to an increased need to base security on widely adopted standards and address the following challenges:

Challenge	Description	Scenario			Priority	Quality
		Cloud only	Hybrid	Mobile		
Info. 1 Ensure data privacy in the cloud	Explains the role of data protection regulations and how they are supported in the cloud				Very high	Mature
Info. 2 Safeguard information at the cloud service provider (CSP)	Discusses how to evaluate whether your company's information is secure at the CSP, concerning, for example, availability, loss prevention, or protection against unauthorized access				Very high	Mature
Info. 3 Safeguard information on mobile devices	Targets the challenge of keeping company data secure on mobile devices				Very high	Enabled
Info. 4 Prevent accidental information disclosure	Focuses on how to minimize risk of disclosure in situations where employees accidentally share the document with people who lack authorization for a particular document – whether they are inside or outside the company				Medium	Enabled
Info. 5 Manage information across applications	Deals with the issue of ensuring that users have the same authorizations for the same business data, no matter in which of the many business applications it resides				Medium	Evolving
Info. 6 Manage keys for users and devices in the cloud	Introduces ideas to prevent CSPs from managing or knowing your private keys, even if they run services for you				Medium	Evolving

Note: Each challenge is labeled alphanumerically so that the information challenges may be quickly identified throughout the document.

1.3.2 Securing Interactions

To embrace cloud and mobile solutions, the company network has to open up to the Internet. However, handling requests that come in through cloud-based and mobile solutions in real time as securely as if they were part of the company network presents several key challenges summarized below.

Challenge	Description	Scenario			Priority	Quality
		Cloud only	Hybrid	Mobile		
Int. 1 Introduce cross-company processes with cloud service provider	Discusses options to ensure that your business processes operate and are supported end to end, even though the responsibility is spread over various companies				Very high	Mature
Int. 2 Safeguard requests on application level	Focuses on the need of validating electronic requests early in your network on the application level to prevent attacks				High	Mature
Int. 3 Safeguard connectivity beyond proxy infrastructure	Deals with system-to-system connectivity across networks and options to secure this beyond a proxy infrastructure				Medium	Mature
Int. 4 Control incoming requests via staging approach	Introduces approaches to temporarily store certain requests in a kind of quarantine if risk to a business process is detected				Medium	Mature

Note: Each challenge is labeled alphanumerically so that the interaction challenges may be quickly identified throughout the document.

1.3.3 Securing Identities

In the IT world users are modeled by identities that need to be authenticated when they access systems and are then provided with authorizations based on, for example, their assigned roles. In the on-premise world, identity management (IdM) solutions are already standard and user authentication has been simplified by single-sign-on (SSO) mechanisms. Extending IdM solutions and SSO to the cloud and mobile world presents the following key challenges:

Challenge	Description	Scenario			Priority	Quality
		Cloud only	Hybrid	Mobile		
Id. 1 Off-board cloud and mobile users	Targets the problem that cloud systems and private devices are to be accessible from outside company firewalls, which means simply withdrawing company access cards will not prevent system access				Very high	Mature
Id. 2 Onboard and manage cloud users	Deals with issues of how to distribute user and related data, keep logon processes simple and secure, and enable off-boarding procedures				High	Mature
Id. 3 Onboard in the mobile world	Focuses on simplicity and automation of onboarding for mobile apps in order to avoid the risk incurred from performing steps manually, and discusses options to prevent access from arbitrary devices				High	Enabled
Id. 4 Enable central authentication and single sign-on (SSO)	Addresses need for true central cross-system authentication and SSO process to disable user/password logons, which often leads to nonsecure passwords and reuse of passwords				High	Enabled
Id. 5 Integrate external "social" identity provider (IdP)	Introduces approaches to integrate external IdP, for example, from social networks, letting consumers of your products interact with your company without cumbersome registration processes				Medium	Enabled

Note: Each challenge is labeled alphanumerically so that the interaction challenges may be quickly identified throughout the document.

1.3.4 How SAP Addresses Those Challenges

As a trusted advisor and reliable business partner to its customers, SAP takes security very seriously, leveraging standards and processes to build security into its software products from the very beginning. SAP engages in continuous research to be able to develop and implement state-of-the-art architectural concepts to help companies address IT security challenges. For each of the challenges mentioned above, key strategies to address them are shared in detail in this guide. The SAP software products that can help to address these challenges are discussed as well.

2 Introduction and Scope

2.1 MOTIVATION AND CONTEXT

On the one hand, there is constant news about companies of all sizes suffering severe damages from security breaches from increasingly complex attacks. The damage could be either monetary loss or regulatory consequences, for example, from the Sarbanes-Oxley Act or data protection laws.

On the other hand, security vulnerabilities increase with trends towards mobile computing and cloud services (see research papers on the topic, for example, "[Protecting the Cloud](#)"). With each new device or system, their weaknesses add risk to the entire network and thus business operations. But businesses are adopting cloud and mobile anyway for multiple reasons – to achieve more-integrated processes or to enable ubiquitous user access, for example. This forces companies and their business partners to constantly adapt their IT security strategy and concepts to manage their business processes securely.

As a software vendor and cloud service provider, SAP has developed and implemented architectural concepts to address modern IT security needs in its business software. This guide describes the concepts that can help all companies respond to security challenges from emerging cloud and mobile trends. It also explains benefits that can be achieved.

2.2 APPROACH OF THIS GUIDE

This guide divides security concerns into the key building blocks of [securing information](#), [securing interactions](#), and [securing identities](#).

It is important to understand available and widely adopted architectural security key concepts for establishing network zones, having authentication policies, and ensuring authorization. Those enterprise baseline security principles are briefly mentioned for each building block. But your focus certainly is on how to address new security challenges from trends like mobile and cloud solutions. These include how to achieve data privacy, how to securely connect to cloud solutions and mobile devices, and how to onboard and off-board identities.

Past IT topics such as hosting and IT outsourcing provided some similar challenges. This indicates that sound architectural responses can be found. The goal of this guide is to share SAP's learning and enable IT security for business applications in a cloud and mobile environment. For this, proper concepts and their benefits are presented.

The responses focus on business processes and software security for relevant applications. Other layers such as hardware and network, database, operating system, or facility security must be looked at separately.

Even though the listed responses are independent from SAP software, this guide describes how SAP addresses them in its products. You will see how SAP software can support the context of "bring your own device," a focus of many IT departments today.

But before diving into architectural responses, the question remains: how do they fit into an IT security concept?

2.3 THE CHALLENGE OF IT SECURITY

Security is always a joint effort made by the company, its industry, standards organizations, governments, and IT vendors. However, businesses have to make trade-off decisions: functionality versus security, usability versus security, supportability versus security, and profitability versus security. In addition, security requirements depend on local regulations, company-specific IT infrastructure, and processes.

Hence a security concept always needs to be company specific, reflecting a company's risk appetite and its protection goals. Threat modeling and a subsequent assessment of vulnerabilities help to clarify the requirements. A security concept should define suitable policies, processes, education of people, and architecture (tools and technology) to manage IT security along the entire lifecycle of business processes.

Among all these aspects of IT security, there are common elements of an IT security architecture that are applicable to many companies. Recognizing these common elements can help as you define the concept and design for your security strategy.

2.4 MODEL FOR ELEMENTS OF IT SECURITY

To look at IT security holistically, a model is used to describe the process steps of business applications, with steps that can be characterized by asking the following questions:

- “Who does it?” – actors or identities
- “What is done?” – the information that is acted upon
- “How and from where is it done?” – the interaction that occurs to access the information
- “When is it done?” – at what time
- “Why is it done?” – for what reason

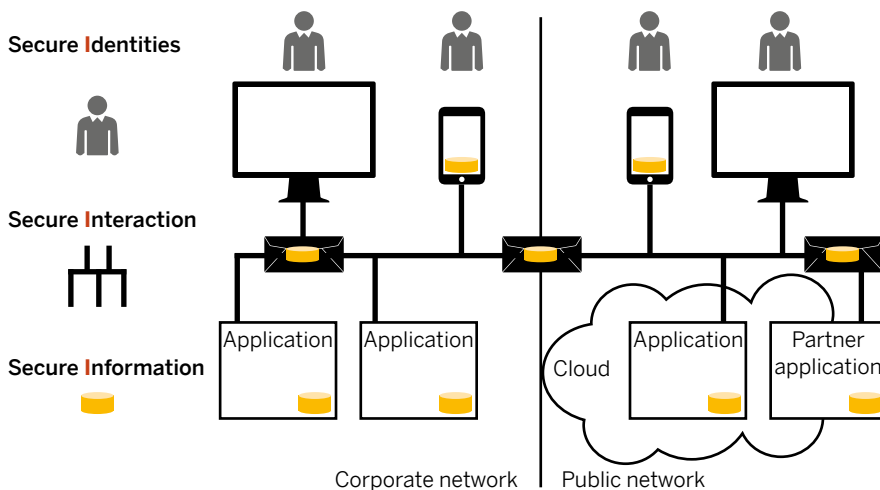
These questions help to structure and identify security challenges and requirements for safeguarding business applications within a company. The first three questions focus on identity, information, and interaction, three important elements of IT security for making business applications secure. They are illustrated in Figure 1.

The questions “When is it done?” and “Why is it done?” are certainly interesting for monitoring and auditing purposes, but relate to managing IT security. Since this is a process rather than an architectural topic, it is not discussed in this paper.

How to establish security in each of these areas has to be addressed in a company-specific concept for managing IT security (see “[The Challenge of IT Security](#)”).

Interestingly, the three elements address the attack targets, as attackers try to obtain or forge identities, analyze how to interact with systems, and hunt for valuable information.

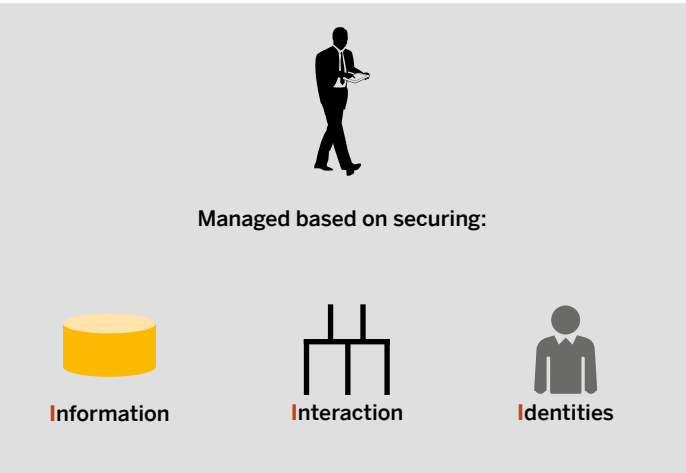
Figure 1: Visualization of Process Step Elements to Be Secured



In addition, this concept helps to put big security topics that you read about into their most important context (see Figure 2).

Finally, it helps to see the binding elements, such as authorizations binding identities and information, as these define what a user can do within an application.

Figure 2: Model for Elements of IT Security



2.5 CHALLENGES BY SCENARIO, PRIORITY, AND SOLUTION MATURITY

To help you determine the relevance of each challenge mentioned in this paper, each is assigned to one of three scenarios (cloud, hybrid, or mobile) as well as given an importance and priority. (For example, a security measure might be designated as mandatory because of the need to conform to applicable regulations.) Challenges are also categorized according to availability of software solutions for a specific challenge. This last criterion gives you an idea of how adequately offerings from software vendors and cloud service providers can address a specific challenge:

- Relevance to scenarios
 - **Cloud-only** environment: Here a company decides to live without any on-premise software for its business applications. However, the business processes can use several cloud services from one or multiple vendors.
 - **Hybrid cloud and on-premise** environment: Here some processes run at least partially in the cloud. This is the typical scenario with most of today's companies. They see an advantage of extending into the cloud without replacing the core and differentiating processes that run in their on-premise software landscape.
 - **Mobile** environment: As mobile offers an additional access channel to business applications, this scenario can coexist with the other two or with a traditional, pure on-premise software landscape. Of course, supporting software like mobile platforms can reside on premise or in the cloud.

Element and Relevant Security Topics

Element of IT Security	Commonly Known Security Topics
Securing information	Data protection and data privacy; data encryption, and message security
Securing interactions	Network and communication security; channel encryption
Securing identities	Key elements of identity and access management
Managing IT security	Governance, risk, and compliance

- Priority based on classification of challenges:
 - **Very high:** The top challenges fundamental for all scenarios that have to be addressed by every company
 - **high:** Challenges that most companies face and for which they request today an integrated solution across different IT vendors
 - **Medium:** All other challenges that add additional security, but whose relevance depends on the individual customer's situation, environment, or business, with each reader determining the degree of relevance for his or her company based on details provided with the challenge
- Qualitative categorization of available software solutions for the challenges:
 - **Mature:** Solid solutions and guidelines that already exist and are used productively by many customers in the market
 - **Enabled:** First solutions that are available and gaining traction, but still being rounded off by IT vendors and customers, with first customers of SAP using productive implementations that cover the key responses of the challenges

- **Evolving:** Initial concepts that exist, with spearheaded usage but no comprehensive response from IT vendors to date, with only customer-specific solutions offered

This categorization allows you to focus on the most relevant challenges when verifying or adapting your security architecture strategy.

This document is intended for use by IT management and enterprise architects. It details security challenges posed by today's cloud and mobile trends and illustrates the response SAP has made to meet these challenges.



3 Reference Concepts

In this section, suitable responses to IT challenges are addressed according to the three security elements highlighted in this guide: securing information, securing interactions, and securing identities. For each security element, the basic architecture is described that every company should already have in place for its traditional on-premise environment. The document then describes in detail the security challenges related to cloud and mobile technologies and the suitable responses.

3.1 SECURING INFORMATION

Let's start with an example. The sales pipeline of a company, employee or customer data, and secret product recipes or blueprints are all examples of information that no company wants to leave insecure. With cloud and mobile on the rise, the information is more easily accessible and is distributed to storages outside of the company's firewalls.

Most of the external regulations focus on governing the confidentiality of information (like data protection laws) or the integrity (like the Sarbanes-Oxley Act). Two other pillars of securing interaction and securing identities are needed, however, as a business needs information to be available, ideally accessible from everywhere by people showing proper electronic identification.

3.1.1 Traditional Baseline for Securing Information

In traditional on-premise business, information is mostly stored on premise and travels mostly within the corporate network. First and foremost, loss-prevention mechanisms and procedures (for example, disaster recovery) must be in place. Only certain information travels via defined channels (e-mail and application-to-application or business-to-business interfaces) to business partners. This requires general assurance of data quality (for example, via virus scans) and data encryption when data is transferred or stored on files or shares.

Authorization concepts within business software systems define who (which role) can access information, which helps ensure segregation of duties, an important component in securing information. Often this is centrally maintained and distributed on premise by identity management solutions, as authorizations form the bridge between identities and information. Authorization concepts must also address the

separation of information according to different levels of sensitivity and importance (such as public, internal, or confidential), for example, into different network areas. This separation additionally helps to secure interaction.

Monitoring and logging procedures can further support information security, audits, and compliance if used when information is accessed and changed. The key points are visualized in Figure 3.

This describes the basic measures to secure information. Additional measures have to be considered to secure information in cloud and mobile scenarios, which are discussed in the following section.

3.1.2 Cloud and Mobile Security Challenges and Responses

Think of employee data that will leave the corporate network for a cloud application handling reward management or a mobile phone on which sensitive company data from e-mail correspondence or company mobile apps is stored. In these cases, your company's information leaves the on-premise world, with other companies, like the cloud service provider (CSP), managing and storing it. Logically, data privacy becomes a key concern, as does the challenge of how to control information security that involves other companies. As mentioned earlier, the fundamentals are data privacy regulation and addressing information security requirements for cloud and mobile environments. Keeping track and staying in charge are important, and include preventing accidental disclosure. This also involves controlling information in a variety of applications and ensuring that each user has exactly the access needed. Last but not least, you should always have the option of retaining full control, which includes maintaining charge of the key management. Figure 4 gives an overview of the challenges involved in safeguarding information.

Figure 3: Key Baseline Elements of Securing Information



Figure 4: Challenges of Securing Information in Cloud and Mobile Environments



Info. 1 Ensure Data Privacy in the Cloud

Cloud only/ Hybrid	Very high	Mature
-----------------------	-----------	--------

To fulfill this challenge, we must start with questions like “Do data protection laws allow employee data to be stored in the cloud?” and “Can my cloud vendor read my data?” In the end, all such questions can be resolved by complying with applicable data privacy regulations. In the EU, the key standard regulations are embodied in the data protection directive 95/46/EC of the European Parliament and of the Council of October 24, 1995. In the United States, the Fair Information Practice Principles from the Federal Trade Commission set forth applicable regulations. There may be additional local or industry-specific laws or regulations you must adhere to. However, regulations of different countries may conflict with each other. For example, the United States has laws embodied in the USA PATRIOT Act¹ that might conflict with data privacy regulations of another country where the data is stored. You need to know the right steps to follow in order to conform with all necessary regulations. Our recommendations advise you to:

1. Determine your own data privacy requirements with regard to the regulations relevant to your company. Make sure you take into account that your CSP is an additional processor and represents an additional storage site for your information.
2. Evaluate how closely the CSP complies with your requirements. Available audit information like ISO 27001 certification provides a good starting point, but analysis should go beyond this. For example, you should also consider how the CSP separates customer data and how authorizations for data access are handled. If the CSP is located in a different country, principles like the [Safe Harbor framework](#) can help. It provides guidance concerning adequate EU personal data protection as required by the European directive 95/46/EC.

3. Satisfy yourself that the CSP is concerned about data privacy in matters that extend beyond your immediate requirements.

By considering these recommendations, you can help ensure data privacy will meet your requirements when using business applications from a cloud service provider.

Info. 2 Safeguard Information at the Cloud Service Provider

Cloud only/ Hybrid	Very high	Mature
-----------------------	-----------	--------

Cloud service providers serve hundreds of customers, and the security investments CSPs make benefit all customers immediately. Because they have a better cost-benefit ratio, CSPs can make much higher investments in security than an individual company. CSPs can also perform security patching in the cloud promptly, while on-premise systems often stay unpatched and, therefore, vulnerable for a long time.

When weighing the advantages a CSP offers, however, the following questions must still be considered: Is there a risk of losing data? What procedures guarantee availability? What disaster protection measures are in place? Is the CSP compliant with applicable regulations, and does the CSP support those regulations for you? Is there a risk of losing confidentiality, for example, due to the country the CSP operates in? The following steps will help you resolve these and other information security concerns:

1. Determine what your company’s security requirements are. This will help you draw up the questions to ask the CSP. Include in your scope of inquiry government regulations such as export control rules, which may prohibit specific company data from being stored outside your country. Know which country the CSP operates from and make sure you are in agreement with having your data stored there.

1. See glossary

- Find out if the CSP complies with standards such as the International Standard on Assurance Engagements (ISAE) No. 3402 and ISO 27001/ISO 27002 standards. This compliance would confirm the reliability of the CSP's internal processes, which would reflect positively on the CSP's ability to safeguard your information. Ask if the CSP conforms with the SSAE 16 (Statement on Standards for Attestation Engagements 16) auditing standard and can provide a Service Organization Control (SOC) 2 report. A positive response to this question would demonstrate that a CSP follows the principles of security, availability, confidentiality, privacy, processing integrity, and privacy.
- Ensure that all your questions – including those concerning physical security, disaster recovery, and authorization concepts for CSP employees – are answered.
- Because CSPs are different legal entities, you should check the details of the service agreements specific to information security. Determine whether you require service-level agreements with the CSP and how to agree on them. But be sure to establish a relationship of trust beyond contractual agreements.
- Perform access validation and encryption of business data beyond what options the device's operating system provides, for bring-your-own devices as well as company devices. You should be able to control the additional settings via server-side configuration, either on an app-specific basis or by on-device data containers shared by several apps. For example, you can protect mobile devices from accessing your software systems with the same password complexity as required for company PCs.
- Keep the option to remotely delete sensitive information via mobile device management software.

All these measures are necessary in order to safeguard information at the cloud service provider.

Info. 3 Safeguard Information on Mobile Devices

Mobile	Very high	Enabled
--------	-----------	---------

Mobile devices are easily lost or stolen and could get attacked by a malicious app. This constitutes a high risk of information exposure, as password protection is usually low for mobile devices. So how can you secure company data on your users' mobile devices? The following measures can help:

- Store as little data as possible on the device. This means that company-developed apps should be designed to store only necessary data on the device. When purchasing apps, this concern should be part of the evaluation procedure. If critical information must stay on the device, it has to be password protected and encrypted, measures that must also cover all backups of the device data.
- Be aware that information could be requested from back-end systems, for example, through a malicious app, via available integration points. Find related recommendations in the ["Int. 2 Safeguard Requests on Application Level"](#) section.

With the increased use of individually-owned and company-owned mobile devices in business, these measures will become relevant to a greater extent. They will help ensure that the information on these devices does not get exposed to unauthorized people.

Info. 4 Prevent Accidental Information Disclosure

Cloud only/ Hybrid/Mobile	Medium	Enabled
------------------------------	--------	---------

With the Internet, e-mail has changed how information is transferred and employees do not always pay enough attention to whom the potential recipients (directly or via forward) of an e-mail might be. With the increase of social networks comes an increase in the risk of critical information leaking. Nowadays, it could happen with a tap on a smartphone or as comments sent through the cloud or mobile apps, not to mention in documents shared with large communities. Additionally, initial load files of cloud applications move past corporate firewalls. So, beyond training your employees, how can you control the information that leaves your business software? These recommended steps will ease this risk:

- Use encryption for all your interactions, including files exchanged with the CSP, for example, for initial load. Your choice is, of course, limited by the offerings of the CSP, but if asked, some CSPs might offer additional encryption options, like usage of Pretty Good Privacy (PGP) encryption with secure file transfer protocol (SFTP). Alternatively, with lower data volumes service-based initial loads can provide the benefit of preventing brute-force attacks on stolen copies of complete files.

2. Classify your information (for example, private, internal, or external) and consider integrating digital rights management (DRM) software directly with your business applications. Ideally, when a document is created for download, it will pass to the DRM tool for encryption before being made available.

The risk that company information will be accidentally disclosed will increase as employees use social media and mobile channels more frequently for business purposes. These recommendations can help reduce accidental information leakage, but can be of only limited help against criminal attacks.

Info. 5 Manage Information Across Applications

Cloud only/ Hybrid/Mobile	Medium	Evolving
------------------------------	--------	----------

Solutions become more fragmented when cloud environments are introduced. If a cloud-based solution for the company's sales staff holds the same opportunity data as the company's customer relationship management (CRM) on-premise solution, both must be protected by similar authorizations. How can this be achieved? The following measures will help:

1. Put in place data flow models and central access-rights documentation. This baseline measure provides needed transparency and operational control to establish a reliable authorization strategy. It is something every company should do. Although it is a well-known and mature measure, it is also costly.
2. Check for new developments for transporting access rights centrally and context-rich definitions of access rights. This could reduce the time required to configure and maintain authorizations in each software landscape.

If the data flow models are not yet transparent enough, an effort must be made to document them again. This work will bring a payoff over time, and not just through increased security levels, but also in supporting your company as it further adapts its business applications.

Info. 6 Manage Keys for Users and Devices in the Cloud

Hybrid	Medium	Evolving
--------	--------	----------

For those customers who manage keys and certificates with on-premise software and distribute them to their users and devices, it may be of interest to them to own the keys for their virtual cloud instances and devices.

Nowadays, CSPs usually know your private keys and control them for you. And there is no technical barrier to copying private keys. As mentioned in "[Info. 2 Safeguard Information at the Cloud Service Provider](#)," having trust in your CSP is essential. However, there is a way to manage your private keys more securely where trust need not be the critical factor.

New solutions are evolving. Hardware partners offer appliances for cryptographic key management, which prevent the CSP or any party other than a special card holder from creating, managing, or reading the keys. The appliance operates in the data center of the CSP after initialization by the card holder and prevents any retrieval of private keys at the CSP. When all key operations go through the appliance, the risk of abuse is greatly reduced.

Concluding Remarks on Information Challenges

The challenges in this section focus on how to comply with data privacy regulations and how to minimize information exposure in the cloud or mobile world. The "very high" challenges of "[Info. 2 Safeguard Information at the Cloud Service Provider](#)" and "[Info. 3 Safeguard Information on Mobile Devices](#)" focus on limiting the amount of information exchanged, ensuring general authorization concepts are in place, and controlling procedures and emergency procedures in the cloud and mobile world. Other challenges are concerned with how authorization concepts and encryption concepts can help safeguard information.

All the measures recommended in this section contribute to increasing the security level of your information, especially when using new cloud and mobile applications. The following section focuses on how interaction channels can be made more secure.

Figure 5: Key Baseline Elements for Securing an Interaction



3.2 SECURING INTERACTIONS

Interactions take place between the company and external networks. This is key for providing information exactly where and when it is needed. In an increasingly interconnected world, businesses expect to access information from everywhere – from home, mobile phones, public Internet access points, the business’s network, and the business partner network – more or less in real time. The baseline elements discussed below, together with the provided responses to recent challenges, can help to create and secure typical defense layers in interaction. The first recommendations provide a baseline for establishing a security architecture that every company should follow. Additional aspects are then considered that take into account cloud- and mobile-related security challenges when securing interactions.

3.2.1 Traditional Baseline for Securing Interactions

Typical scenarios that should be made secure in the traditional world of on-premise-focused software include portal-based self-services that integrate with, for example, enterprise resource planning (ERP) software, or supplier and customer networks via intermediate documents (IDocs).

The typical baseline measure starts with a system landscape model that supports segregation of interactions into firewalled network zones. This includes extra zones for external-facing portal or middleware. Additionally, network-layer security must be in place to technically secure access and transport of data in the network. It is important to be aware that this impacts all

interactions, not just with cloud and mobile applications, and that risks and mitigation paths for the company must be defined.

Application software is used only if it fulfills security standards and is patched in order to avoid known vulnerabilities. Unpatched software that can be accessed via the public network no longer protects information. For external communication, proxies and reverse proxies are the de facto standards. They can hide Web servers and applications to the outside, reduce the number of interaction channels, and perform further services, such as Secure Sockets Layer (SSL) encryption, load balancing, and access control (see Figure 5).

In general, secure interactions are established by means of defense layers. Each zone as well as each technology layer has to contribute to the overall security of interactions and work hand in hand with the other zones and layers.

The following section describes in detail how cloud and mobile interactions can be secured.

3.2.2 Cloud and Mobile Security Challenges and Responses

Let’s start again with an example. Think of the mobile apps used by sales staff that has direct access to the back-end CRM software or of the cloud applications that extend the human capital management (HCM) on-premise software. Both require data exchange. Both serve as examples of the modern need to open up internal systems to the external network, while ensuring the interaction can be handled securely. Figure 6 shows key challenges involved in securing this kind of interaction.

Figure 6: Challenges of Securing Interactions for Mobile and Cloud Solutions



These challenges go beyond technical connectivity, which involves general network technology, proxies, load balancers, virtual private network (VPN) endpoints, firewalls, and the like. Technical connectivity is part of the above-mentioned interaction baseline and is often managed by a different IT department. The challenges described here and in the following sections focus on application connectivity, for example, what is necessary in terms of application-level middleware.

Int. 1 Introduce Cross-Company Processes with CSP

Cloud only/ Hybrid	Very high	Mature
-----------------------	-----------	--------

With critical business applications running in the cloud, reliable real-time integration with on-premise software is important. In the world of on-premise software, companies manage all issues in connectivity on their own, while in the cloud they rely on the CSP and telecommunication and network companies to do this. Who is then responsible for fixing a bug or blocking an attack to keep the processes going? To answer this question, you need to:

1. Have joint procedures with the CSP on how to solve unexpected integration errors or security threats. These procedures need to be well understood and practiced to ensure a fast resumption of normal operation.
2. Support interaction procedures through service agreements between the companies. Concepts like nonrepudiation – meaning both sides can show what messages were really sent and received – further help to determine interaction issues and trigger corrective action.

These recommendations are process-oriented. Nevertheless, there should be an application infrastructure in place that allows recurring issues to be detected and resolved quickly.

Int. 2 Safeguard Requests on Application Level

Hybrid/ Mobile	High	Mature
-------------------	------	--------

With the steady increase in incoming request traffic to the on-premise software from cloud and mobile solutions, there is also an increase in attack surface. Pure technical checks on the network layer are not enough. For example, the checks cannot perform a thorough input validation based on application information. So how can real-time requests from cloud and mobile be handled securely? These measures can help:

1. Introduce protective measures like protocol switches, deep packet inspection, or thorough input validation, including context information, to ensure that request fields are within defined constraints depending on their origin. Such functionality can be offered via application-level gateways (ALGs).
2. Investigate where to do which application-level checks. An ALG in a more exposed network zone prevents unwanted requests from getting to the application and its higher secured network zone. On the other hand, the ALG, and with it the application context, might be easier to spy out. Hence application-level checks should also be offered directly in the application. At that point, it is an individual trade-off decision based on the information at risk as to which checks to perform in a pure ALG or a middleware or via application-internal input validations and checks.

These checks on the application level are necessary in order to detect attacks targeted beyond the network level.

Int. 3 Safeguard Connectivity Beyond Proxy Infrastructure

Hybrid	Medium	Mature
--------	--------	--------

The biggest issue with cloud services is that they live in a different network outside company firewalls. How can you best connect your application software systems to the cloud? The minimum security need, as for other outside connectivity, is a proxy infrastructure, but are there options that add to the proxy infrastructure?

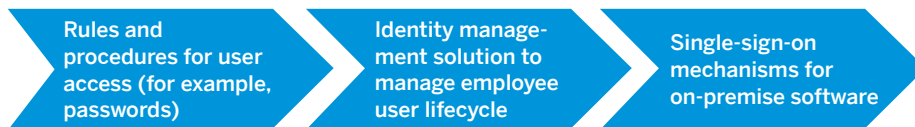
Check whether your CSP offers connectivity services. Preferably, cloud-to-on-premise connectivity is initiated from on-premise software. This avoids having to open on-premise firewalls for inbound calls. Typically a permanent secure interaction path between cloud and business software systems should be established. The path should also protect against interception.

Int. 4 Control Incoming Requests via Staging Approach

Hybrid/ Mobile	Medium	Mature
-------------------	--------	--------

Even if the measures described above are in place, there might be special circumstances in which companies might not trust the load coming through the external network from the cloud or mobile world. In that case, they may want to block certain interactions from reaching business systems in case of security

Figure 7: Baseline Elements of Securing Identities



alerts. One way to achieve this is a mailbox-like interaction via staging areas. Ideally messages are collected in dedicated queues, allowing businesses to selectively decide on what to block from reaching the back-end system and allow other business processes to continue running. Depending on security needs, such approaches can be achieved via middleware solutions inside a dedicated network zone or even outside the company firewall. True mailbox approaches do not allow real-time communication and thus are limited to selected scenarios, for example, when you want to stop information requests coming from the outside that have (basically) no business impact if they remain unanswered.

3.2.3 Concluding Remarks on Interaction Challenges

How a company responds to the cloud- and mobile-related security challenges described above, including usage and configuration, will differ depending on the company's security needs. For example, a company might choose to live without additional cloud connectivity components or staging approaches.

3.3 SECURING IDENTITIES

All the challenges and recommendations mentioned in the previous sections focus on securing information and interaction channels. In order to establish security comprehensively, we also have to safeguard the identities that are used to access in-

formation via interaction channels, the subject of this section. Information is accessed through an interaction channel, which is typically authenticated based on identifying attributes and credentials that determine the identity. So what is needed to secure the identity for all requesters (device, other server, or user)?

Central storage of identities could be one answer, as it is also often propagated for other master data. With no replication, one indisputable owner and record of truth exists and no changes need to be propagated. This reduces the attack surface and makes it easier to secure. This however hinders availability and performance, which is why applications often require some local storage for user and access data. The following covers both central and local storage of identities. Measures that companies should already have adopted in traditional on-premise environments will be discussed first, followed by a discussion of new challenges and responses for securing identities in cloud and mobile environments.

3.3.1 Traditional Baseline for Securing Identities

Companies initially struggle with concepts for granting employees and partners access to the multitude of business software systems. They manage them and guarantee that a user will be blocked as soon as he or she, for example, leaves the company or changes position.

A typical baseline security concept for identification usually covers an on-premise software world. Employees typically make up the bulk of users. Employees might access the company network from outside, for example, when working from home. Business partners might access systems like a supplier portal.

In this context, key security anchors are business process-driven identity management (IdM) solutions used to onboard, distribute, manage, and off-board users. For this reason, an IdM solution ideally provides a complete view on which software systems a user has access to. IdM software is complemented by user and password rules as well as single-sign-on mechanisms (see Figure 7).

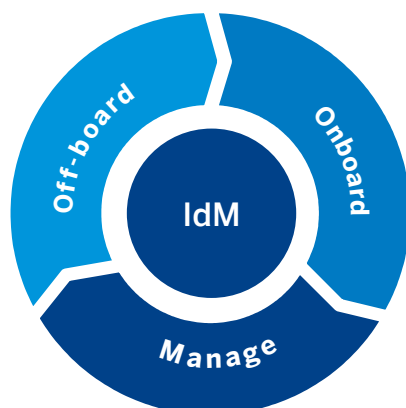
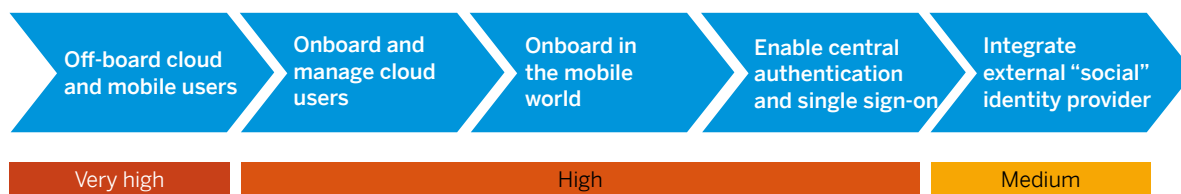


Figure 8: Challenges of Securing Identities for Cloud and Mobile Solutions



IdM solutions can manage the onboarding, management, and off-boarding of users. The relevant identity data is periodically synchronized from leading software systems (for example, HR software for employees), stored (for example, in a Lightweight Directory Access Protocol [LDAP] directory), and distributed to other business software systems.

In authentication policies, companies can define password complexities, “forgotten password” processes, when two-factor identification (for example, smart cards such as RSA SecurID cards) must be used, and if and how single-sign-on will be used. As IdM solutions often have an integrated identity provider (IdP), they can support SSO functionality. If an employee signs in with an IdP with whom a relationship of trust has been established, a token or certificate is granted with which the employee gains access to all business software systems. In today’s IT landscape, there are a variety of SSO mechanisms, many vendor specific (for example, logon tickets used by SAP software). Hence IdPs often do not work in cross-domain, cross-network zones, or across vendors.

Extending SSO functionality to cloud and mobile applications will become a key requirement for hybrid landscapes, which is discussed next.

3.3.2 Cloud and Mobile Security Challenges and Responses

Let’s look again at an example. Think of sales staff that accesses the cloud application for customer management via mobile devices. The application interacts on behalf of the sales rep directly with the company’s on-premise ERP software to determine, for example, pricing. In such a scenario, the identification process involves mobile and cloud solutions and requires service-based, on-behalf logon, as the cloud application accesses the ERP software.

Hence the need for secure identification increases, still based on the two pillars of IdM and SSO. Interestingly, an SAP customer survey on product experience from 2011 showed SSO to be the most important topic for product experience in hybrid landscapes. A look at specific challenges you will face in a modern cloud and mobile environment concerning SSO and IdM and suitable responses will be of help (see Figure 8)

In a modern infrastructure, users belonging to various roles, such as employee, partner, or customer, must be managed. The users need to access a variety of applications running on premise, in the cloud, or on a mobile device. Reliable and immediate off-boarding becomes important, as otherwise information might still be accessible from the Internet or a privately owned cell phone. A good onboarding and managing process for cloud and mobile users is certainly a necessary precondition. Single-sign-on mechanisms are crucial in such a landscape for usability in order to prevent a multitude of passwords per user. Especially for consumers, it must be considered that external IdPs from social networks, for example, may be used. This will be discussed later.

Id. 1 Off-Board Cloud and Mobile Users

Cloud only/ Hybrid/Mobile	Very high	Mature
------------------------------	-----------	--------

Let’s start with one of the most important challenges when safeguarding identities in mobile and cloud environments: off-boarding cloud and mobile users. Reliable and often immediate blocking of user access to cloud or mobile apps is needed. Ideally this should happen without manual workflows. Off-boarding of employees is especially critical, for example, in case of termination of work relations. While in a pure on-premise software world, withdrawing entry cards and remote logon devices is sufficient, cloud and mobile applications might remain accessible.

To achieve user off-boarding:

- 1) Classify users into categories like employees, partners, end customers, and consumers
- 2) Establish real-time access withdrawal for critical categories:
 - Establish real-time interfacing between leading software systems (like human capital management software for employees) and IdM solutions, as well as cloud software and mobile device management platforms. This will help ensure the immediate blocking of users for cloud solutions and deregistration of appropriate mobile app, device, and user combinations.
 - Be careful when buying or developing mobile apps that access applications via technical users. Here you need to be able to deregister the app-user-device combination immediately (for details on the registration concept, see “[Id. 3 Onboard in the Mobile World](#)”). Alternatively, you should have a process in place that remotely deletes apps from mobile devices to prevent further system access. Remote wiping has further benefits, like securing information that exists on the device, but it is often more difficult to enforce, especially for noncompany devices.
- 3) Define reliable off-boarding for other user categories. Real time might not be necessary, however no application should remain accessible indefinitely. User categories like consumers can even have legal rights that stipulate by when their access and data has to be removed. Additionally, no automated onboarding procedure should grant access rights to off-boarded users.

Off-boarding can be extremely time-critical whereas onboarding (discussed below) can be planned and, because it is a high-frequency process, should be automated.

Id. 2 Onboard and Manage Cloud Users

Cloud only/ Hybrid	High	Mature
-----------------------	------	--------

Streamlined onboarding and user management reduces total cost of ownership. From a security point of view, the simplicity reduces administrative mistakes and prepares for the off-boarding process. How should you distribute and manage user- and other person-related data in parallel? Which IdPs

are needed for which tasks in a cloud environment? What is needed to prepare for immediate off-boarding? Here are some recommendations:

1. The IdP is needed to replicate necessary user-related data. Do not use it for further person-related business data, as the IdP often has no semantic knowledge about the sensitivity of business data. Use instead your master-data management solution to replicate other employee and business partner data.
2. The system landscape should have a main IdP managing potential further IdPs
3. Additional IdPs or IdP tenants can add value, for example:
 - Separation of different kinds of users, for example, consumers and employees
 - Usage of a central cloud IdP (in addition to a main on-premise IdP) for employee data. Then no trust relationships need to be maintained between the main IdP and each cloud application. In some cases, the cloud IdP does not even need to have the user data stored locally, but can function as a proxy.
 - Sometimes applications might require specific IdPs be added to the landscape, which could then be used to achieve the benefits mentioned above. Generally, integration with the main IdP should be targeted. Here standards like the system for cross-domain identity management (SCIM) can reduce the effort to onboard and manage the user data.
4. Solutions that make only the necessary attributes available to the IdP (for example, user name and e-mail address) are preferable for login. The more business data of the user is managed in an IdP, the more one needs to invest in continuous protection and distribution of the attributes.
5. Your applications should be configured in a way that a user can only log in via the IdP. If a direct login to the application with user name and password without the IdP SSO is impossible, there is no need for password procedures. Additionally off-boarding needs to deal just with the main cloud IdP and not with potentially countless applications.

As described above, IdPs are an essential component in securing identities in cloud environments. Let's look now at how to onboard securely and efficiently in the mobile world.

Id. 3 Onboard in the Mobile World

Mobile	High	Enabled
--------	------	---------

One aspect to onboarding mobile devices and onboarding and configuring mobile apps is how to avoid manual steps. Additionally there is the challenge of avoiding access from unknown or arbitrary mobile devices. Measures to achieve straightforward, nonmanual configuration of mobile devices and the blocking of unwanted mobile devices include:

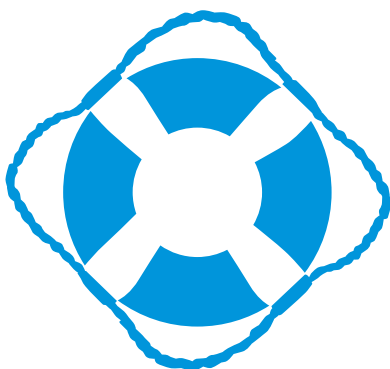
1. For mobile apps with out-of-box configuration, there are two options:
 - A company-owned app store, which already has the pre-configured apps accepted for the users
 - A company-owned mobile platform, which offers support for configuration and onboarding, for example, via a general on-device client or via central configuration services
2. To avoid unwanted access to back-end software, use mobile app registration (for example, via a mobile platform or device management solution). This typically works by having users log on to a central registration service, where the user, device, and mobile app ID combination is stored. It could also be supported by device clients or apps that enable central configuration and possible storage of authentication credentials for all business apps.

As explained above, in the mobile world you need the combination of user, device, and mobile apps for secure onboarding. These onboarding processes are a prerequisite to accessing all relevant business applications. But how can you ensure secure authentication and SSO functionality for all applications in mobile and cloud environments for all new and existing employees? This will be discussed next.

Id. 4 Enable Central Authentication and SSO

Cloud only/ Hybrid/Mobile	High	Enabled
------------------------------	------	---------

The core challenge in the cloud is how to enable central authentication and SSO for all cloud applications. In the mobile world, apps can live without their own authentication, provided the device is secured by a good central authentication. However mobile apps often interact with business applications. This requires an authentication process between applications in the context or on behalf of a specific user.



Security vulnerabilities increase with trends towards cloud services and mobile computing. With each new device or system, its weaknesses add risk to the entire network and thus business operations.

To achieve vendor-independent and cross-network authentication and SSO procedures you should:

1. Strategically move to software supporting Security Assertion Markup Language (SAML) 2.0 for front-end authentication. SAML 2.0 offers rich functionality that builds on a trust relationship between an IdP and applications. An existing IdP (for example, an on-premise one for employee data) can be extended to support cross-network and cross-vendor SSO, if it supports SAML 2.0. SAML 2.0 allows true vendor-independent cross-network and cloud SSO. It can be based on existing IdPs with SAML 2.0 support. An additional benefit is that SAML 2.0–asserted sessions can serve multiple authentication requests and can be the basis of single logout.
2. Understand your needs for service-based authentication. For each applications-interaction, is the context of the initially triggering user needed and provided for authentication in the request-receiving system? Here concepts like principal propagation (see the “Glossary” section) can help. It is also important to understand what technology or protocol the interaction is based on, for example, if SOAP or Representational State Transfer (REST) is being used for the service interaction.
3. Determine the right service-based authentication solution. In the Web services world of SOAP and Web Service Security (WSS), SAML assertions are often adopted and supported to enable authentication. For integration based on REST and Open Data Protocol (OData), Open Authentication (OAuth) 2.0 is the emerging standard of software companies. OAuth provides additional benefits, like constrained delegation to limit authorizations of an app accessing on behalf of a user to the absolute minimum (least-privilege principle).

The measures to perform vendor-independent and cross-network authentication and SSO are based mainly on open standards like SAML and OAuth.

Id. 5 Integrate External “Social” Identity Provider

Cloud only/ Hybrid	Medium	Enabled
-----------------------	--------	---------

With billions of identities residing in social networks like Facebook, you might have asked yourself, why not leverage these identities to streamline consumer access to your systems? You might want to attract consumers to your company products through, for example, communities, forums, or smartphone apps. This can easily be enabled with today’s cloud and mobile solution offerings. Consumers will not like cumbersome self-registration processes, for example, if you request identity and logon details. Nowadays, many consumers are constantly logged on to their preferred social network (not just social networks like Facebook, but also consumer marketplaces such as Amazon, eBay, and associated services such as PayPal). This could be incorporated into the authentication process:

1. Determine for which of your applications you could trust an external IdP to provide the identity data. This will result in different trust levels, depending on your applications’ security needs.
2. Evaluate whether you can set up trust relationships between your application and the relevant social IdP, for example, by using SAML 2.0. You can also incorporate your own IdP by establishing a special trust level for the social IdP and certain identities that you want to accept, including mapping to possibly differing identities in your IdP. This way, if there are reports of a security breach with the social IdP, you can efficiently prohibit SSO via that IdP by revoking the trust in your IdP.

Consumers will enjoy their choice of seamless SSO using their social logon or having additional data privacy by creating a separate logon. This can extend reach and customer satisfaction and at the same time allow you to continue collecting your required consumer data, such as e-mail addresses and names.

With all these challenges and IT responses to safeguard information, interaction channels, and identities, you might want to know how to realize these recommendations with available solutions from SAP. That is the topic of the next section

4 SAP Products

4.1 SAP SOFTWARE FOR HIGH QUALITY AND SECURITY

In addition to helping its customers meet the security challenges discussed above with robust, effective measures, SAP is committed to delivering software that meets highest quality and product security standards. Through its internal development processes, SAP builds in product security right from the beginning. This is accomplished not just by developing specific security functionality, but also by making sure that all SAP software fulfills a broad range of architectural, design, and security requirements before it ships.

SAP approaches security in its products holistically and does not see its responsibility as software manufacturer end with the delivery of high-quality, well-tested software. SAP extends its responsibility to include offerings for security-related support, security guidelines and recommendations, security products and functionality, specialized security consulting teams, and a network of specialized partners.

The following sections focus on each of the three key elements of the security model: information, interactions, and identities. They discuss how the broad portfolio of SAP offerings addresses the security challenges and responses discussed in the sections above. Mentioned first are the typical SAP offerings for on-premise environments that help address security aspects in on-premise and hybrid environments. Next, details are provided on the security offerings from SAP for the cloud, relevant for cloud-only and hybrid environments. Last but not least, security-related offerings from SAP for the mobile environment are provided.

To conclude, a discussion is provided on how these concepts can be realized in a bring-your-own-device (BYOD) scenario.

4.1.1 For Securing Information

Let's look first at offerings that secure information for hybrid environments.

On-Premise Offerings from SAP for Hybrid Environments

All SAP software supports information security in various ways. One key element is encryption, which becomes more impor-

tant when you open up your on-premise systems for interaction with hybrid environments. The [SAP NetWeaver®](#) technology platform supports standard security functions like SSL, Secure Network Communications (SNC), and Secure Store and Forward (SSF). The [SAP NetWeaver Identity Management](#) (SAP NetWeaver ID Management) component not only helps to secure identities; by allowing you to centrally manage access rights for everything from workstations to company parking garages, it also helps you directly secure information.

To protect files that leave an SAP solution automatically, one can apply [digital rights management](#) encryption. Further, SAP proved in a [sample implementation](#) that this can be achieved by connecting a digital rights management solution like Active Directory Rights Management Services from Microsoft to the SAP NetWeaver technology platform. This increases security in hybrid environments, for example, when a document is shared in a cloud-based collaboration tool.

Securing Information in the Cloud

All cloud solutions from SAP focus on data protection and highly [secure data centers](#). The U.S.-based cloud offerings from SuccessFactors and Ariba, two SAP companies, are formally part of the Safe Harbor Program (see challenge "[Info. 1 Ensure Data Privacy in the Cloud](#)"). This program is committed to the stricter data protection principles set forth by the European Union. As for information security, cloud solutions from SAP and operating centers run by SAP have a variety of certifications. SAP, SuccessFactors, and Ariba all successfully completed SSAE 16 audits. Additionally, SAP conducts regular external penetration tests. An overview of security information is available from [SAP](#). SAP also provides security information for the SAP Cloud portfolio, including information on software from [SuccessFactors](#) and [Ariba](#).

SAP provides to customers of its cloud solutions extensive service agreements that establish, for example, service-level agreements for availability. These agreements also clearly demonstrate SAP's obligations concerning access control, input and transmission control, and data separation. All these aspects contribute to greater understanding about how information is secured.

All cloud solutions from SAP support modern encryption techniques, which are discussed in the security guides for cloud solutions from [SuccessFactors](#), for cloud suites such as the [SAP Business ByDesign®](#) solution, and for software from Ariba. Encryption offerings for file integration also exist. For example, files in software from SuccessFactors can be transferred via secure FTP and encrypted with PGP. Additionally, the SAP Jam social software platform classifies groups into, for example, public and private. This is, in itself, a ready-to-hand method to protect against accidental information disclosure.

Securing Information in Mobile Solutions

[SAP Mobile Platform](#) can secure information using client file encryption and user credential checks for applications accessing information. Encryption and one password protecting critical information stored on the device is enabled by the data vault concept. This concept is built into normal mobile solutions from SAP and is generally available when developing apps on SAP Mobile Platform

The [SAP Afaria® mobile device management solution](#) is available as on-premise software and as a cloud offering based on Amazon Web Services (AWS). To fortify security for information stored on devices, the solution uses strong encryption. It also enables corporate security to log on and report security activity on the device. Most important, the software can remotely lock app access and delete app-specific information based on confirmation. SAP Afaria can be used to enforce power-on passwords and policies like usage of strong passcodes.

SAP also offers SAP Afaria in the cloud and partners with trusted telco operators and system integrators to offer additional managed mobility services. Cloud offerings for mobile solutions are especially interesting, as mobile devices are already outside the company network, and the entire topic of enterprise mobility can be left to expert companies that can automatically update mobile security for you.

The [SAP Mobile Documents](#) solution gives employees secure access to documents instantly on PCs, laptops, smartphones, and tablets. It works closely with standard corporate document management software. The mobile app enables businesses to maintain control over corporate data on all devices to support compliance, and it uses encryption, authentication, and assigned role-based rights. It is offered in the cloud or as on-premise software.

Security offerings from SAP focusing on mobile solutions are rounded off by the [SAP Mobile App Protection solution by Mocana](#). This solution “wraps” data protection and access control features around an app – without any manual changes or coding. It can add security to all company apps to help protect information on all managed and unmanaged devices.

All SAP solutions mentioned in this section can help safeguard information in hybrid, pure cloud, and mobile environments. Let's take a look now at SAP solutions suited for safeguarding interaction channels.

4.1.2 For Securing Interactions

Let's look first at offerings for securing interactions in hybrid environments.

On-Premise Offerings from SAP for Hybrid Environments

With SAP NetWeaver Process Integration (SAP NetWeaver PI) technology, SAP offers professional middleware that can enable cloud integration. The software natively supports application-level gateway functionality – for example, protocol switches and input validations – and the staging-area approach, which can be provided via the messaging queues. SAP development teams follow development guidelines, that enable them to produce business applications that support general input validation. This can increase application security in times when applications are opened up to external access from cloud applications or mobile devices.

Products like [SAP NetWeaver Gateway](#) technology can be deployed as a separate hub. As the name indicates, SAP NetWeaver Gateway offers application-level gateway features, such as protocol switches and input validation. The software can also function as a security layer between mobile and on-premise environments and between cloud and on-premise environments.

Securing Interactions in the Cloud

For integration with cloud applications and social applications in the cloud, SAP offers the support of reverse-proxy-based integration for its cloud products, including those from SuccessFactors as well as SAP Business ByDesign. SAP provides a [connectivity service](#) that can act as a connectivity provider for integration, for example, with SAP HANA® Cloud Platform, the SAP open-standards platform-as-a-service (for details, please refer to the related [white paper](#)). Additionally, a [technical connectivity guide](#) focuses on cloud applications based on SAP Business ByDesign, providing detailed information on integrating cloud applications.

SAP is continuously extending its cloud integration services based on SAP HANA Cloud Integration technology. The technology offers typical middleware features also known from on-premise products from SAP such as SAP NetWeaver PI and SAP Data Services software. Similarly, it offers application-level functions and a staging approach. But most important, together with the on-premise middleware offerings from SAP, it gives customers the choice of having all integration on premise, in the cloud, or a combination of both. Non-SAP middleware software can also function as an application-level gateway or as a staging area for SAP business applications.

Securing Interaction in Mobile Solutions

As a leader in mobile solutions, SAP provides advanced interaction security with [SAP Mobile Platform](#). The platform provides proxy functions. Its connectivity components can help ensure that inner firewalls need not be opened for inbound calls. On top of this, the platform can function as a staging area. In addition, the [SAP Mobile Secure set of solutions](#) can help ensure that devices are patched promptly with the latest software. Last but not least, SAP recommends building mobile apps based on REST-based services that can access business software via [SAP NetWeaver Gateway](#), which enables it to provide application-level gateway features.

All these SAP solutions help safeguard interaction channels. Suitable SAP solutions to safeguard identities – the last key element of our security model – are explained next.

4.1.3 For Securing Identities

Identity management is the heart of securing identities, and SAP's approach to it is twofold:

- Support the customer's choice of identity management product
- Offer an SAP solution in order to support the best integration possible with SAP software

On-Premise Offerings from SAP for Hybrid Environments

First of all, in the world of on-premise software, customers can use their existing identity management solution for standard SAP software. The software can be used in hybrid environments by integrating with cloud identity providers based on standards like SAML 2.0. With [SAP NetWeaver ID Management](#), SAP offers its own identity management software for SAP customers to manage identities for their SAP and third-party software.

[SAP NetWeaver ID Management](#) provides a wide range of connecting software to supply SAP and third-party software (including LDAP directories) with identity-related data. In this way, core business software such as human capital management software can transfer, for example, employee data to SAP NetWeaver ID Management. [SAP NetWeaver ID Management](#) manages the data centrally and distributes the data. SAP NetWeaver ID Management also provides connecting software

Front-End-Based Single Sign-On for SAP® On-Premise Software

	SAML 2.0	Kerberos	X.509 Certificates
SAP NetWeaver® technology platform and the ABAP® programming language	Yes, since version 7.02	Yes: SAP NetWeaver Single Sign-On application, 2.0	Yes
SAP GUI	n/a	Yes, with SAP NetWeaver Single Sign-On or a certified partner product	
SAP NetWeaver technology platform and the Java programming language	Yes, since version 7.20	Yes	Yes
SAP® BusinessObjects™ Business Intelligence platform, 4.0	Yes, via SAP NetWeaver technology platform as Java-based trusted authentication	Yes	Yes, via SAP NetWeaver technology platform as Java-based trusted authentication

to SAP HANA software. Integration with [SAP solutions for governance, risk, and compliance \(GRC\)](#) and the [SAP NetWeaver Single Sign-On](#) application is supported. Integration with the SAP NetWeaver Business Process Management component provides state-of-the-art features for the authorization approval workflows business owners use for role assignment.

Identity federation with a SAML 2.0 identity provider and a security token service using the WS-Trust 1.3 standard (with WS standing for Web services) is also included. This makes it easy to interact with cloud applications in hybrid environments. WS-Trust can distribute identities to cloud IdPs and support IdP proxies. SAP NetWeaver Single Sign-On is a specialized on-premise SSO solution offering secure login, enterprise SSO, central IdP, and support of trusted authentication mechanisms, smart cards, and two-factor authentication. The solution additionally supports key standards like SAML and the Kerberos security protocol. It provides the option of issuing short-lived X.509 certificates.

Securing Identities in the Cloud

Cloud platforms from SAP, SuccessFactors, and Ariba support SAML 2.0. With any of this software, applications can connect to an IdP using, for example, an on-premise solution such as SAP NetWeaver ID Management. This is enabled by configuring the cloud application as a SAML 2.0 service provider and setting up a trust relationship.

SAP offers the [SAP ID service](#), which provides a range of features, including:

- Central storage for identities related to all on-demand applications
- Single sign-on between SAP on-demand applications and integration with third-party on-demand applications
- Central management of identity information, including user information, such as name, descriptor, e-mail address, and passwords
- Synchronization of user accounts to and from on-demand target systems
- Runtime functionality for user authentication, single sign-on, and trust management

It is the basis for managing identities on SAP HANA Cloud Platform and for SAP Community Network and supports single sign-on. To further support the SAP ID service, other cloud solutions from SAP offer additional integration for easier user provisioning, for example, a central employee integration option in software from SuccessFactors. It is left to the customers to decide how far to adopt the SAP ID service for their tenants in SAP HANA Cloud Platform. SAP already uses it for a variety of cloud-based solutions, such as the SAP Cloud for Travel mobile app and SAP Jam.

Additionally SAP is promoting adoption of the OAuth 2.0 open standard for authorization for components that provide or consume REST or OData services.

Securing Identities in Mobile Solutions

Mobile app registration processes are supported in both the on-premise and the cloud versions of the enterprise and consumer editions of [SAP Mobile Platform](#). With [SAP Afaria](#), IT can manage devices remotely, enforcing security policies, controlling what software is installed, and wiping data from the device if it is lost or stolen or the employee leaves the company. SAP Afaria supports the central configuration of apps on the device. SAP promotes adoption of OAuth 2.0 to support the communication of mobile apps with back-end software or a cloud service on behalf of a user.

The SAP solutions suitable for safeguarding information, interactions, and identities have just been described. Next, we turn to how these SAP solutions can be used for the specific use case of BYOD based on the concepts discussed in “Reference Concepts.”

4.2 REALIZING BYOD: AN EXAMPLE

BYOD is a highly relevant topic for many companies. Often employees want to work with just one mobile device and prefer their own device to company offerings. Yet supporting a BYOD policy entails urgent security implications from a legal aspect – privacy laws and country-specific regulations. There are security implications from the HR perspective – clear onboarding

and off-boarding procedures. And there are considerations from an IT perspective, with the company needing to retain control of company information. IT can only support this with country-specific BYOD policies that, for example, specify the approved models and operating system versions and ensure a company's security requirements are met. The latter is especially important as the device and noncompany apps cannot generally be maintained by the company. IT also requires an infrastructure for mobile device management.

To review the ground rules IT managers must consider when establishing a BYOD policy, please consult the white paper from Sybase, an SAP company, [*An IT Manager's Guide to Managing Personal Devices in the Enterprise*](#). While that paper discusses issues that have been known for some time, we discuss below architectural challenges BYOD policies bring with them today, and how these challenges were resolved by SAP and SAP customers.

The use case is discussed sequentially. We start with onboarding, move to securing interactions between the device and the business software, and conclude with a discussion of how to manage company data on the device.

4.2.1 Onboard User, Device, and Apps

Let's start with onboarding. It's the initial challenge for each employee device. It is important to manage the apps each user has on each user's device and how to introduce user-friendly app configuration.

As BYOD policies get adopted country by country, SAP Mobile Platform can be used to register the combination of user, device, and app ID. It is critical to have a place – a company app store or a download place – that makes available the company-approved mobile apps that can be used to access the company software.

SAP Afaria is a device management solution with a client on the mobile device. This can help to share configuration data between the company apps (if they were designed to work with a device management solution) and to provision the connect information to the devices.

4.2.2 Manage Mobile Access to Company Software

After onboarding, secure interaction between the device and the business software becomes the focus. Gateway functionalities that protect interaction between mobile apps and the company's on-premise or cloud-based software are offered via SAP NetWeaver Gateway. Additional interaction security can be achieved by registering all interaction on a central mobile platform. This has the advantage that you can centrally deregister a device or user with no worries that an individual app will still be able to access back-end software with a user and password combination. SAP Mobile Platform offers secure connectivity via its components (for example, the relay server and relay server outbound enabler) for company devices as well as non-company devices.

A device management solution like SAP Afaria can help detect and prevent access if devices are not on the latest patch level or if they were tampered with, for example, a device that was subjected to iOS jailbreaking (for example, via the [*SAP Mobile Secure rapid-deployment solution using SAP Afaria or via the SAP Mobile App Protection solution by Mocana*](#)). Certainly denying unpatched devices access to company software is problematic in multinational corporations, as device security patches are often not synchronized for the entire world. However, depending on the criticality of back-end accesses, it is a valid option.

4.2.3 Manage Company Data on the Device

As company data could well end up on the device, it is not enough to know the device-user-app combination and secure the interaction with back-end software. Data on the device needs to be protected from unwanted usage. While data encryption can be handled by the apps, and SAP Afaria can enforce usage of a strong password to enter the device, the question is, what happens if a device is lost or an employee leaves the company?

In many countries a valid approach is to include in BYOD policies the rule that the company has the right (and ability) to remotely wipe the entire device if it is lost or stolen. However, this is not an option in the European Union. For the EU, remote wiping must happen on the mobile app level. For all major platforms, [SAP Afaria](#) supports a device wipe; for enterprise mobile apps, it renders the app and the data unusable. It can enforce encryption of the data on the device for apps and support significant further device management functions.

SAP Afaria is also available as a [cloud edition](#). Specifically for company e-mails, contacts, and calendars on the private device, SAP is partnering with NitroDesk to offer such security measures as PIN enforcement, encryption, and remote wiping functions. However, information can easily be posted in communities or shared via services such as Dropbox. This is certainly not a mobile-specific risk, but a risk for all computers or devices that connect to the Internet. Because the company ultimately loses control over the data, employees must be made aware of possible issues and be equipped with company-approved and mobile-accessible solutions, for example, for sharing data. In this case, a good alternative to Dropbox is [SAP Mobile Documents](#), which was developed specifically for enterprises and offers similar options for sharing data, but leaves the enterprise in charge.

The SAP solutions mentioned in this section discuss present time. However, because requirements and technology are constantly evolving, especially in the mobile area, future challenges are addressed briefly in the following section.

4.2.4 Overcome Further Challenges

SAP is continuously working on further improvements, for example, working with partners on how to have one entire container for all business-related apps and data on the mobile device. SAP continuously enhances SAP Mobile Platform and SAP Afaria. And SAP works closely with device manufacturers to further extend enterprise support. As an example, SAP has partnered with Samsung and now offers broad “[Samsung SAFE](#)” support

5 Conclusion and Outlook

The previous sections provided answers to key challenges that companies face in establishing IT security in traditional software environments as well as for cloud-based and mobile solutions. The challenges and responses were organized according to a model that provides a comprehensive look at all security aspects of business applications. The three key elements of that model are: securing information, securing interaction channels, and securing identities. These challenges were mapped to specific scenarios (cloud-only, hybrid, and mobile), priorities in terms of general requirements (for example, compliance regulations), and quality in terms of maturity of available software products for that specific challenge.

Below you will find a summary of the challenges discussed, along with the recommended responses and benefits you can expect.

Challenge	Recommended Response	Benefit	Scenario			Priority	Quality
			Cloud only	Hybrid	Mobile		
Securing Information							
Info. 1 Ensure data privacy in the cloud	1) Know relevant regulations and determine your compliance needs 2) Review certifications of your cloud service provider (CSP) 3) Satisfy yourself as to the CSP's commitment to data privacy	Informed confidence that your CSP can and will meet your compliance needs				Very high	Mature
Info. 2 Safeguard information at the cloud service provider	1) Determine your information needs 2) Ensure that the CSP fulfills process standards 3) Get answers from CSP and draw up service agreements 4) Build a relationship of trust with CSP	Fulfillment by CSP of agreed-on requirements so you reap needed cloud benefits, such as fast security patching				Very high	Mature
Info. 3 Safeguard information on mobile devices	1) Minimize offline storage of information and use encrypted storage containers 2) Protect back-end systems from unwanted information retrieval by mobile devices 3) Be able to manage remotely 4) Be able to wipe remotely	Protection against typical risks, such as lost or stolen devices				Very high	Enabled
Info. 4 Prevent accidental information disclosure	1) Ensure all interaction with CSP is encrypted, including initial data load files 2) Classify your information and integrate digital rights management software	Protection of information through encryption at rest and in transit				Medium	Enabled
Info. 5 Manage information across applications	1) Use data flow models and document your access rights centrally 2) Stay up-to-date with developments of transportable access rights and context-rich definitions of access rights	Transparency in documentation and groundwork for central definition to simplify solution and save costs in future				Medium	Evolving
Info. 6 Manage keys for users and devices in the cloud	Know how your CSP protects encryption keys and, if needed, store your encryption keys in a solution the CSP cannot access	Full control of your encryption keys				Medium	Evolving

Challenge	Recommended Response	Benefit	Scenario			Priority	Quality
			Cloud only	Hybrid	Mobile		
Securing Interactions							
<u>Int. 1 Introduce cross-company processes with cloud service provider (CPS)</u>	1) Establish ability to perform processes jointly with CSP 2) Establish service agreements and concepts like nonrepudiation, when possible, to support interaction	Fast resumption of joint operations				Very high	Mature
<u>Int. 2 Safeguard re-requests on application level</u>	Use application-level gateway functionality	Processing of requests only after application context validation				High	Mature
<u>Int. 3 Safeguard connectivity beyond proxy infrastructure</u>	Initiate cloud connectivity service from on premise	Closed firewalls for inbound calls				Medium	Mature
<u>Int. 4 Control incoming requests via staging approach</u>	Use staging approach, ideally with message queues	Ability to delay or stop certain messages in staging area without impacting business systems operation				Medium	Mature
Securing Identities							
<u>Id. 1 Off-board cloud and mobile users</u>	1) Classify users in categories 2) Define off-boarding that uses identity management (IdM) and mobile solutions and is: - Reliable for all user categories - Real time for critical categories like employees	Ability to block central users immediately without manual workflow				Very high	Mature
<u>Id. 2 Onboard and manage cloud users</u>	1) Define main identity provider (IdP) 2) Define distribution rules per user category 3) Follow master data and IdM principles 4) Store only necessary attributes with IdP 5) Disable user name and password login for apps	Minimized data duplication and establishment of well-controlled processes in preparation for easy off-boarding				High	Mature
<u>Id. 3 Onboard in the mobile world</u>	1) Use company mobile platform or app store 2) Use mobile app registration	Automatic onboarding and blocking of non-compliant devices				High	Enabled
<u>Id. 4 Enable central authentication and single sign-on (SSO)</u>	1) Adopt SAML 2.0 for front-end authentication 2) Define service-based authentication needs 3) Determine a fitting service-based authentication standard for your company	Cross-vendor and cross-network SSO; standards-based authentication and SSO				High	Enabled
<u>Id. 5 Integrate external "social" identity provider</u>	1) Determine whether integration is needed 2) Establish concept of trust levels and minimize trust relations	High consumer adoption of your apps, for example, due to easy first-time logon				Medium	Enabled

Personal data and business information is always in the center of security thinking, hence data privacy and information security were the first topics addressed. However, in a highly interconnected world, where information needs to be accessible from everywhere to all properly identified users, it was pointed out that there are ready-to-use products for securing identities and securing interaction across your entire landscape of business software, be they SAP or non-SAP, cloud, mobile, or on-premise solutions. Specifically, the importance of connectivity providers and application-level gateway functionality was pointed out for securing interaction. Process-driven IdM and SSO (across the entire business software landscape) concepts were detailed for securing identities.

A comprehensive company-specific security concept has to cover more aspects than just technology and architecture. Required security processes within the company must also be drawn up. Further, SAP provides information and help on processes of secure software development, and conforms to its own internal product standard for security in developing its products. Information on best practices to [help partners and customers with secure application development](#) is externally available. Another aspect is that software must be made available via reliable sources. (At SAP, we have the [SAP Service Marketplace](#) extranet and [SAP Store](#)). Additionally, support is required from security specialists via [consulting services](#) (login required), [support services](#), [security notes](#), and [patch processes](#) for the implementation, configuration, and operation phases of

software development and usage. These examples focus mostly on the application lifecycle aspects. SAP offers holistic solutions for GRC, such as the SAP Risk Management application and the SAP Access Control application, which can further help you determine and manage the risks that a security concept addresses.

Last but not least, each company must prepare its people throughout the organization to follow the company security concept. Well-trained and knowledgeable employees are the security force needed to operate the security processes and technology.

SAP offers solutions that support the concepts discussed in this paper in order to help customers run their business processes securely between their on-premise SAP and non-SAP software, cloud solutions from SAP, and mobile devices managed and integrated via mobile solutions from SAP. SAP is continuously investigating security aspects in architecture with respect to all recent trends, such as mobile and cloud. SAP will further adopt concepts as well as target development of solutions for upcoming security challenges to bring the utmost security benefit to customers. When you need the latest security information, always check [SAP Community Network](#) and the [security page](#). These pages also point you to security solutions, security services, and details and guidelines on the [security of SAP offerings](#).



In an interconnected world, information security must span different legal entities and countries. It must cover cloud service providers, network providers, and your own company. This calls for security based on widely adopted standards.

6 Find Out More

6.1 FURTHER INFORMATION ON SECURITY AT SAP

Here is a comprehensive list of information sources from SAP if you would like to learn more about IT security. Listed first are general entry points for security. Next are links to information that supports making decisions for a secure architecture (for example, security products from SAP and white papers). Last but not least, links to information are included that support you on an operational level as far as security is concerned.

6.1.1 General Information on Security at SAP

Entry points to the SAP Web site for the topic security:

- Overall security entry page:
www.sap.com/pc/tech/application-foundation-security/software/security-solutions-overview.html
- Entry page to the approach to security promoted by SAP:
www.sap.com/pc/tech/application-foundation-security/software/security-at-sap/index.html
- Security entry page at SAP Service Marketplace:
<https://service.sap.com/security>
- SAP Community Network entry page for security:
<http://scn.sap.com/community/security>
- Information on data centers hosted by SAP:
www.sapdatacenter.com
- Entry page at the Ariba Web site: <http://trust.ariba.com>
- White paper from SAP and SuccessFactors:
www.successfactors.com/content/dam/successfactors/en_us/resources/white-papers/sap-cloud-security.pdf

6.1.2 Information About Designing a Secure Architecture

Information on SAP core solutions and products for IT security:

- General information on:
 - Product road maps: <https://service.sap.com/roadmap>
 - SAP NetWeaver Identity Management:
www.sap.com/pc/solutions/tech/application-foundation-security/software/identity-management/index.html
 - SAP NetWeaver Single Sign-On: <http://www.sap.com/solutions/tech/application-foundation-security/software/single-sign-on/index.html> and an informative blog: <http://scn.sap.com/community/netweaver-ssso/blog>
 - SAP Access Control: www.sap.com/solutions/tech/application-foundation-security/software/access-control/index.html
 - SAP Risk Management: www.sap.com/solutions/tech/application-foundation-security/software/risk-management/index.html

- Cloud connectivity: <http://scn.sap.com/community/developer-center/cloud-platform/blog/2012/10/05/sap-cloud-connector-110-available-on-sap-service-marketplace>
- SAP NetWeaver Gateway: www.sap.com/solutions/tech/business-process-management/software/connectivity-framework/index.html
- SAP NetWeaver Application Server component:
<http://www.sap.com/pc/tech/application-foundation-security/software/application-server/index.html>

Technical connectivity guide for cloud applications based on SAP Business ByDesign: <https://websmp201.sap-ag.de/~sapdownload/011000358700000894852012E> (requires login for members of SAP Community Network)

- General overview of SAP Mobile Platform: www.sap.com/solutions/tech/mobile/software/solutions/platform/overview.html and detailed information on older releases: <http://infocenter.sybase.com/help/index.jsp>
- SAP Afaria, SAP Mobile Documents, SAP Mobile App Protection by Mocana, and services to manage enterprise mobility: www.sap.com/solutions/tech/mobile/software/solutions/device-management/overview.html and detailed information on older releases: <http://infocenter.sybase.com/help/index.jsp>
- SAP solutions for governance, risk, and compliance (GRC): www.sap.com/pc/analytics/governance-risk-compliance.html
- SAP Mobile Secure rapid-deployment solution: <http://scn.sap.com/community/rapid-deployment/blog/2013/10/08/managing-mobile-devices-in-a-world-of-jailbreaking>

Security white papers from SAP:

- White papers on secure development, secure configuration, and security services: <https://websmp108.sap-ag.de/securitywp>
- White paper on cloud connectivity service: <http://scn.sap.com/docs/DOC-34458>
- At the SuccessFactors Web site, search white papers on security: www.successfactors.com/en_us/resources.html
- Sybase white paper on employees' personal devices: www.sybase.com/files/White_Papers/IT-Mangers-Guide-WP.pdf

SAP blogs on digital rights management:

- <http://scn.sap.com/community/security/blog/2012/10/10/digital-rights-management-for-documents-in-sap-systems>
- <http://scn.sap.com/community/security/blog/2013/02/05/digital-rights-management-proof-of-concept>

Blog on Cloud Security at SAP

- <http://scn.sap.com/community/cloud/blog/2013/08/07/the-1-2-3-of-cloud-security-at-sap?source=email-emea-sapflash-newsletter-20130909>

Social media research hub created by Oxford Economics and SAP on cloud platform trends:

- <http://cloudplatformtrends.com>

Developing apps as a partner or customer – with chapter on security: <http://bestbuiltapps.sap.com>

Paper on enterprise mobility, security concerns, and avoidance:

- www.sap.com/solutions/tech/mobile/software/solutions/device-management/security.html
- Learn about mobile security concerns and avoidance: <http://www.sap.com/bin/sapcom/downloadasset.mobility-security-concerns-and-avoidance-pdf.html>

SAP Insider article on SSO in the cloud:

<http://scn.sap.com/docs/DOC-20016>

SAP and Samsung SAFE:

www.sap.com/news-reader/index.epx?pressid=20512

6.1.3 Information About Supporting Secure Operations

Security guides for SAP products:

- For Ariba: http://trust.ariba.com/PN_Policies/
- For SAP Business ByDesign: search via <https://www.sme.sap.com/irj/sme>
- For SuccessFactors: search white papers on security via www.successfactors.com/en_us/resources.html

Information on the SAP Security Optimization service, for example, on how to maintain a constant, automatic security check of the current configuration: <https://service.sap.com/sos>

Security services at SAP from the services catalog:

[https://serviceportfolio.wdf.sap.corp:443/b2b_spm/init/\(layout=6_4_6_1&uiarea=1\)/do?forward=viewarea&startupareaid=0000000219&language=EN&shop=SPM_SBLIVE](https://serviceportfolio.wdf.sap.corp:443/b2b_spm/init/(layout=6_4_6_1&uiarea=1)/do?forward=viewarea&startupareaid=0000000219&language=EN&shop=SPM_SBLIVE)

Information on the security notes from SAP:

See entry page: <https://service.sap.com/securitynotes>

Information on the security patch process at SAP:

See the list of frequently asked questions on SAP Community Network: <http://scn.sap.com/community/security/blog/2012/03/27/security-patch-process-faq>

Technical connectivity guide for cloud applications based on SAP Business ByDesign: <https://websmp201.sap-ag.de/~sapdownload/011000358700000894852012E>
(requires login for members of SAP Community Network)

7 Glossary

A2A	Application-to-application: interaction that occurs between applications at one company
ALG	Application-level gateway: software layer that provides security measures like protocol switches, deep packet inspection, and input validation. Application relates here to the application layer, which is an abstraction layer used in communication protocols, for example, described in the Open System Interconnection model or the Transmission Control Protocol/Internet Protocol (TCP/IP). Be aware that the application-layer definitions vary in scope, however the layer is always above lower layers such as the transport layer, which establishes connectivity.
AWS	Amazon Web Services: Amazon offers virtual machines in the cloud on which SAP solutions can be deployed.
B2B	Business-to-business: electronic transactions between one business and another, for example, between a supplier and a retailer
BYOD	Bring your own device: term that describes the recent trend of employees bringing personally owned mobile devices to their place of work and using those devices to access privileged company resources such as e-mail, file servers, and databases
CSP	Cloud service provider: software company that offers software as a service over the Internet
Data vault concept	A concept within SAP® Mobile Platform to securely store data on a device
Deep packet inspection	A form of computer network packet filtering that examines the data part of a packet as it passes an inspection point, searching for protocol noncompliance, viruses, spam, intrusions, or defined criteria to decide whether the packet may pass or if it needs to be routed to a different destination*
DRM	Digital rights management: not in the context of controlling or preventing copyright infringement of sold content (this was in use in the music industry), but to protect and secure company documents from accidental open distribution
Dropbox	A secure container, where an item (for example, files) can be deposited. Dropbox Inc. is a company that offers a file hosting service with the name Dropbox. An alternative to the Dropbox service, especially in the enterprise context, is the SAP Mobile Documents solution.
EU Directive 95/46/ED	The core European Union directive on protection of individuals concerning processing of personal data
FTP	File transfer protocol: protocol for uploading and downloading files

GRC	Governance, risk, and compliance: security-related topics that each company faces and that are addressed by dedicated software products, such as SAP solutions for governance, risk, and compliance
IdM	Identity management solutions: solutions that help companies centrally manage user accounts (identities) in a complex system, multivendor landscape
IDoc	Intermediate document: standard SAP format for electronic data interchange between systems
IdP	Identity provider: an entity that manages identity information for principals and provides authentication services to other trusted service providers
IdP proxying	Allows an IdP to proxy the authentication requests from a service provider to another IdP, where the user has already authenticated himself or herself
ISAE 3402	International Standards for Assurance Engagements (ISAE) No. 3402: a definition for a global assurance standard for reporting on controls at a service organization, which is also relevant for cloud services
ISO/IEC 27000 series	A series of information security standards providing best-practice recommendations; all organizations are targeted and audits exist for many standards of the series.*
Kerberos	Widely adopted authentication protocol using symmetric cryptography, which was developed at the Massachusetts Institute of Technology
LDAP	Lightweight Directory Access Protocol: software protocol for managing directory data, in other words, enabling anyone to locate organizations, individuals, and other resources, such as files and devices, in a network
Nonrepudiation	Term meaning that both sides can show what messages were really sent and received, which serves as an aid to determine interaction issues and trigger corrective action
OAuth	Open authentication: an open standard for authorization; this key method provides clients access to a server resource on behalf of a resource owner.
OData	Open data protocol: a resource-based Web protocol defining operations using HTTP verbs (GET, PUT, POST, and DELETE) and identifying resources using a standard uniform resource identifier (URI) syntax
OP	On premise: term that implies the traditional setup that hardware and software is owned and operated by each company inside its firewalls

Penetration test	Evaluation of network security by simulating an attack from external or internal threats*
PGP	Pretty good privacy: popular program to encrypt and decrypt data traffic over the Internet
Power-on password	Password required each time a device is turned on (for example, notebook, tablet, or mobile phone)
Proxy (server)	Computer network service that acts as an intermediary for accesses between network zones, for example, between the Internet and an intranet
REST	Representational state transfer: like SOAP, REST is another style of software architecture with which Web services can be realized.
RSA SecurID	Mechanism developed by Security Dynamics (now RSA, The Security Division of EMC) for performing two-factor authentication for a user to a network resource*
SAFE	Samsung for Enterprise: program developed by Samsung designed to alleviate the security concerns of enterprises and employees using mobile devices for business purposes**
Safe Harbor framework	Framework developed between U.S. and EU governments to allow U.S. companies to comply with EU Directive 95/46/ED
SAML	Security Assertion Markup Language: an open standard-based framework for exchanging authentication and authorization information, with an identity provider who issues a security token (also known as SAML assertion) to enable authentication at the service provider
SAP ERP HCM	SAP ERP Human Capital Management solution: solution that offers a complete and integrated set of tools to help manage people effectively
SCIM Standard	System for cross-domain identity management standard: standard created to simplify user management in the cloud by defining a schema for representing users and groups and a REST API for all the necessary create, read, update, and delete (CRUD) operations*
SLA	Service-level agreement: an agreement that defines the attributes for service products (for example, maintenance or hotline) that have been agreed upon with the customer in service contracts and specifies certain parameters, such as response time, availability time, and system availability
Smart card	Any pocket-sized card with embedded chip; for security use cases the chip can provide cryptographic algorithms, for example, enabling two-factor authentication.
SNC	Secure network communications: interface allowing secured communication connections between SAP software components; strong authentication, integrity protection, and privacy protection may be provided.
SOAP	Simple Object Access Protocol: protocol that specifies exactly how to encode an HTTP header and an XML file so that a program in one computer can call a program in another computer and pass it information
SOX	Sarbanes-Oxley Act: U.S. law of 2002 that requires management and auditors of public (and to a lesser extent private) companies to help ensure that their financial statements are accurate and that their internal controls are effective

SSAE16-SOC2	Statement on Standards for Attestation Engagement: measure that targets auditing for compliance with ISAE 3402. Service Organization Control 2 (SOC2) focuses on the nonfinancial trust service principles of security, availability, processing integrity, confidentiality, and privacy.
SSF	Secure store and forward: an interface that allows SAP software to protect data and documents using digital signatures and encryption
SSL	Secure Sockets Layer: Internet standard protocol developed by Netscape used to secure communications across the Internet between a network-layer protocol (for example, TCP/IP) and an application-layer protocol (for example, HTTP)
SSO	Single sign-on: mechanism that eliminates the need for users to enter passwords for every system they log on to, so users need only authenticate themselves once and then log on to all of the systems that operate in the single-sign-on environment without further intervention
Two-factor authentication	Authentication method that requires two factors, for example, a smart card and a password
USA PATRIOT Act	Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001: U.S. counter-terrorism legislation limiting protection of individuals and their personal data*
VPN	Virtual private network: private data network that makes use of the public telecommunication infrastructures and maintains privacy through the use of a tunneling protocol and security procedures
WSS	Web Service Security: an extension to SOAP to apply security to Web services, it was published by the Organization for the Advancement of Structured Information Standards (OASIS).*
WS-Trust	An extension to WSS dealing with trust relationships and the issuing, renewing, and validating of security tokens*
X.509 certificate	A digital certificate issued by a certification agency following the X.509 standard for issuing certificates for a public key infrastructure

* Excerpted from www.wikipedia.org articles on the respective topic

** Excerpted from www.samsung.com/global/business/mobile/solution/security/safe-samsung-for-enterprise

Contact Information

To learn more about the security approach used at SAP, or to discuss security with SAP experts, please contact us at SAP_Product_Architecture_Communications@sap.com.

www.sap.com/contactsap

CMP 23740 (13/12)

© 2013 SAP AG or an SAP affiliate company. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP AG. The information contained herein may be changed without prior notice.

Some software products marketed by SAP AG and its distributors contain proprietary software components of other software vendors. National product specifications may vary.

These materials are provided by SAP AG and its affiliated companies ("SAP Group") for informational purposes only, without representation or warranty of any kind, and SAP Group shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP Group products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP AG in Germany and other countries.

Please see <http://www.sap.com/corporate-en/legal/copyright/index.epx#trademark> for additional trademark information and notices.



The Best-Run Businesses Run SAP™