SAP Technical Brief

ESTABLISHING TRUST FOR E-BUSINESS: SAP® TRUST CENTER SERVICE

Open IT infrastructures are increasingly replacing closed systems in the e-business world. People want one-step business with seamless process chains to eliminate the gaps in integration that waste time and money. Companies are involving business partners more and more in their internal processes to streamline their business activities. This openness offers all kinds of new opportunities while also raising certain issues. For example, how can you be sure that the person accessing your systems, who claims to be your partner, is really your partner?

JOIN THE TRUST COMMUNITY

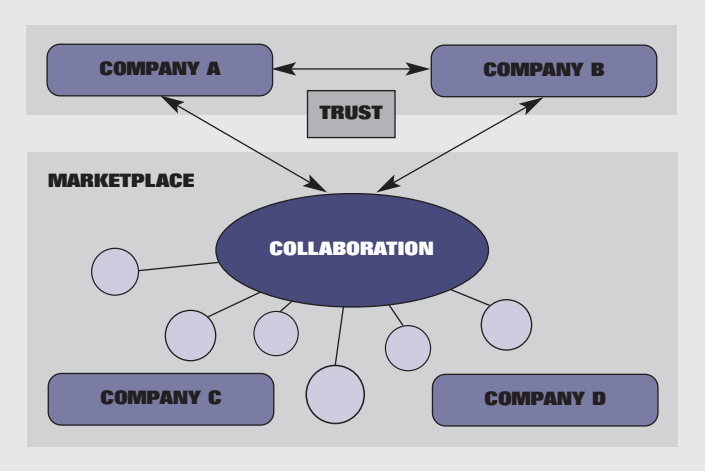
Trust is the basis of every business relationship, and it is particularly important when collaborating with customers and partners over the Internet. Of course you trust your partners – but you need to know that your supplier's sales employees, who have access to your retail system, are who they say they are when they register. The traditional methods of checking identification face-to-face – for example, presenting an identity card – have to be applied in the online world. People or machines involved in e-commerce must be able to prove their identities with the appropriate means. This applies to encrypted, companywide communication between servers as well as external users needing access to internal back-end systems. The identity proof that is furnished must be sufficient and verifiable. In the Internet world, just as in the real world, an administration function is required that issues identity cards and, if necessary, blocks them. In addition, an administrative body is required, similar to a local office that registers residents, to register users and check their identities before forwarding their applications to the issuing authority.

The solution is to use digital certificates. Digital certificates are issued by a trustworthy certification authority, and they link the natural identity of a person or an IT system with a digital identity. The digital identity consists of a cryptographic key pair with both a public key and a private key that are mathematically dependent on one another. The public key is freely accessible, but only the certificate owner knows the private key. Digital certificates give you a secure infrastructure for reliably authenticating users and systems. This infrastructure is known as public-key infrastructure or a trust network.

When a number of companies trust a particular certification authority, the certificates are used not only within the company, but also for interenterprise relationships. A trust community develops where business is conducted efficiently beyond corporate boundaries. It is easier to exchange information and seize opportunities in a trust community, and you can also avoid the costs that arise when you and your business partners use different data formats and media. Digital certificates may be used for digitally signing documents and for transferring encrypted data. They are the most powerful authentication technology available, and all standard security protocols and applications support them.

SAP TRUST CENTER SERVICES

How does a trust community develop? Ideally, you build on an existing infrastructure. With some 15,000 customers worldwide, SAP is in an excellent good position to build a trust community. The SAP Trust Center Service issues digital certificates free of charge to employees and systems of SAP customers, thereby creating a reliable network of trusting relationships between participating companies. The benefit is clear: All members of the trust community can rely on the certified identity of the systems and users who have a certificate for authentication purposes. All of them trust the SAP Trust Center Service as a certification authority.

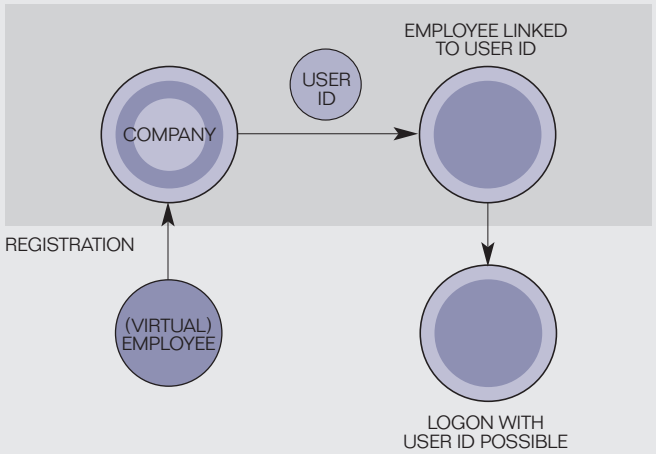


The SAP Trust Center Service issues certificates based on a reliable registration procedure. The registration authority software for servers resides on the SAP Service Marketplace, so you can apply for a certificate for your server by logging onto SAP Service Marketplace. Individual users can apply for certificates directly from their mySAP.com® solutions.

When a user or system applies for a certificate a registration authority first checks if the technical name assigned to the user or the system matches the actual identity. The registration authority can use information from existing registration processes in the mySAP.com solutions at your company. This means that if you're already running a mySAP.com solution that has integrated user administration – such as mySAP Financials – the registration authority can use its successful assignment of user accounts. Certain requirements must be met. For example, each user name must be assigned to a real person; test systems with generic user names are not permitted. When anyone attempts to register a server via the SAP Service Marketplace, the registration authority checks to be sure the person applying for the certificate is really acting on behalf of the company and that the company in fact possesses the domain name for the server – like www.sap.com.

After checking the identity of the applicant, the registration authority forwards the certificate request to the SAP Trust Center Service. When the SAP Trust Center issues the certificate, the identity of the user or system is linked to the digital identity. Invalid certificates – for example, if an employee leaves the company – are revoked in the SAP Service Marketplace. The SAP Service Marketplace distributes to the SAP trust community a certificate-revocation list containing the serial numbers of invalid certificates. Members of the SAP trust community can choose how frequently to receive the updated list.

STRONG REGISTRATION FOR INTERNAL AND VIRTUAL EMPLOYEES



Server Certificates
If your business performs transactions that transfer valuable information over the Internet to your business partners, it is essential for this information not to get into your competitors' hands. How do the servers know they are communicating with the right counterpart and not with an imposter? The answer is simple: The servers exchange certificates that uniquely identify them beyond corporate boundaries and enable the encryption of the transfer path with Secure Sockets Layer (SSL).

The registration authority for server certificates resides on the SAP Service Marketplace. The SAP Trust Center Service issues certificates for servers running SAP Web Application Server, which is the underlying technology of nearly all mySAP.com solutions as well as certificates for Web servers from other manufacturers.

SAProuter Certificates for Support Connections
The SAProuter is part of a firewall system and controls connections between internal and external networks. You can obtain special server certificates to validate Internet connections set up for support purposes between your company and SAP via the SAProuter. In general the certificates are used to authenticate servers for transferring encrypted data within mySAP.com using the interface Generic Security Services API (GSS-API). You can obtain SAProuter certificates free of charge through the SAP Service Marketplace.

The SAP Passport
It is not just systems that communicate in an interenterprise environment. You, your employees, and the employees of your customers and partners interact through portals and require personal access to information and applications. You need a quick, simple, and secure authentication process to enable convenient transaction processing in your complex business relationships.

If you pass the inspection during the registration process, the SAP Trust Center Service issues a certificate in the form of an SAP Passport. This certificate is your digital identity card for the Internet, and it identifies you as a member of the SAP trust community. With your certificate, you can access Internet services that accept the SAP Passport as proof of identity. The passport is very easy to use. You do not need another password. In addition, systems can be configured to grant automatic access to external users who possess an SAP Passport when they log on.

You can obtain your SAP Passport through any of the solutions of the mySAP.com e-business platform. mySAP™ Enterprise Portals, mySAP™ Exchanges, and cross-industry solutions such as mySAP™ Financials and mySAP™ Customer Relationship Management offer automated registration procedures. Once the SAP Trust Center Service receives your registration information, it automatically issues your SAP Passport. You need no additional hardware or software at the front end. The standard cryptographic functions of common browsers are used for the procedure, which is based on Internet standards.

SAP AG
Neurottstraße 16
69190 Walldorf
Germany
T +49/1805/34 34 24
F +49/1805/34 34 20
www.sap.com

SAP uses the SAP Trust Center Service internally, too. Certificates have already been issued for 30,000 employees worldwide, which gives them single sign-on access to the more than 1,000 relevant SAP internal systems. Customers and partners are also able to log on to the SAP Service Marketplace using their SAP Passport and benefit from the advantages of a certificate-based, single sign-on mechanism. They no longer have to provide their user names and passwords repeatedly to the various Web servers of the SAP Service Marketplace, because the browser and Web server automatically exchange the certificate via an SSL connection.

With your SAP Passport, you enjoy the following benefits:

- Your SAP Passport provides secure access to all internal systems that support a certificate-based log-on. Log-on tickets are a secure alternative for systems not supporting certificates.
- Using your SAP Passport, you can obtain authentication for you and your employees to access external systems via the Internet.
- You can have more than one passport, which means you and your employees can enjoy the benefits of the certificates at work, at home, and when traveling. It is simple and quick to apply for a new certificate from a different workplace.
- The SAP Passport gives partners easy access to systems. They no longer have to log on with user names and a password. The SAP Trust Center Service takes over the complex procedure of assigning passwords and checking identities.
- The SAP Trust Center Service allows you to use digital signatures for transactions – so you can electronically confirm a booking, for example.

The SAP Trust Center Service provides you with a complete public-key infrastructure that is available worldwide and at a fraction of the cost you would incur to build up your own infrastructure. Within the integrated SAP trust community, doing business with partners who also use the SAP Trust Center Service is quicker, more efficient, and secure.

E-business cannot function without a secure foundation of trust. Unlike other public-key infrastructure services, which usually do not have such a wide-ranging network of connections, the SAP Trust Center Service uses existing relationships between SAP and its customers and business partners to create a solid foundation for business processing over the Internet – the SAP trust community. You can interact with your business partners using the broad security infrastructure of mySAP.com in an environment that ensures you have secure, efficient processes that go beyond your corporate boundaries.

The SAP Trust Center Service complies with open Internet standards, such as SSL and the certificate format X.509, and can therefore be used together with other public-key infrastructure solutions.

Outlook

New functions are planned for the future to complement existing services. For example, a time-stamp service can prove that data was available at a particular time. The integration of smart cards offers additional security for sensitive company information. Strong certificates can be used on the server side in the future – for example, for digital signatures. Such certificates meet highest security requirements because they are saved to a cryptoboard that cannot be manipulated.

50 040 535 (01/10/13)