Data sheet

FUJITSU PalmSecure truedentity

Biometric Unified Identity based on human palm vein and global trust services - Fujitsu PalmSecure truedentity is used for the mutual authentication of both service and user. Depending on the usage scenario, the security level is scalable.

Convenience and trust go together

If users want to access online services or protected information, they have to prove their identity. This is currently done by entering a password in connection with a user name or by means of 2-factor authentication on the basis of a chip card in connection with a PIN. These procedures, however, involve the risk that cards can be copied and revealed in order to then be misused in conjunction with a PIN.

This is exactly where the technology of PalmSecure truedentity comes into play - it creates an inseparable connection between the user's identity and his uncopiable identifier, while the service in use also has to identify itself to the user.

PalmSecure truedentity is based on the technology of the new German identity card and the technical guidelines of the Federal Office for Information Security (BSI), and combines these with the biometric procedure of palm vein authentication and a substantial improvement of the usability. Depending on the intended use, the technology supports various security levels and the ability to use already existing.

A key service (eID-Server), the so-called identity provider with its intermediary role during mutual authentication, is integrated into the communication. It confirms the correctness of the service identity to the user and takes on the task of identifying the user for the service provider. Depending on the security level to be implemented, the user's identity data can be stored in a secure provider database, managed by the truedentity Server. The identity data is transmitted using special, highly-secure transfer methods.

Trusted biometric identity – all in one

PalmSecure truedentity technology is based on the use of personal palm vein geometry as a biometric feature, which is also stored securely for comparison in a provider database. The personal palm vein geometry of the owner is recorded during the creation of a user's truedentity ID via Fujitsu PalmSecure and is compared with the user's palm vein (1:1 comparison) prior to reading the identity data. Any misuse through stolen identities is detected and prevented in advance.

Biometric procedures have the advantage that they are linked to a person and make the entry of PINs and passwords superfluous. Compared to other biometric procedures, the advantage of Fujitsu's biometric palm vein detection is that it is very secure. This is because, for one thing, the palm vein pattern is hidden from view in the hand and a scan only works when blood is circulating through the vein (bio detection).

The pattern with more than 5 million reference points is very complex and the subsequent validation is 100 times more precise than, for example, identification by fingerprint and even identical twins can be distinguished from each other. Furthermore, a palm vein is a biometric feature which does not change over the course of a lifetime.

Features and benefits

Main features	Benefits
Fujitsu PalmSecure truedentity technology stack	
■ Consists of client and server components ■ Different authentication scenarios that can be consolidated ■ Mapping of various security levels ■ Use of mutual authentication	■ Easily adaptable for specific applications ■ Various business models: Self-operation of the truedentity server with maximum control as a provider or use of truedentity as a service via a connection to a provider
User-centric authentication of possible tokens	
■ Only the user grants access to his/her identity data ■ The truedentity infrastructure confirms the authenticity of the identification data presented	■ Prevents the possibility of authentication data theft by merely not having to transmit this data to the service provider. This results in security and the potential to save costs. ■ Compliance with data protection regulations
Comprehensible user authenticity	
■ Combination of truedentity technology with the biometric palm vein scanner PalmSecure ■ PKI technologies in connection with cryptographic methods ■ Protection of communication through electronic certificates	■ Implementation of multi-factor authentication on the basis of biometric methods ■ Exchange of identity data only between trustworthy and authorized communication partners ■ Prevention of man-in-the-middle attacks
Great flexibility	
■ Support of all relevant authentication scenarios ■ Adaptability of the technology to the required authentication protection level ■ Use of different ID Mediums through standardized ID document ■ Combination with secure hardware solutions	■ Fujitsu PalmSecure truedentity allows the standardization of logon procedures to different systems (web applications, operating systems (domain logon), ...) ■ Scalability of the supported protection levels through the variation of product and process features
Use of protocols for official documents	
■ Support for the internationally accepted protocols PACE and EAC ■ Compliant with the relevant Technical Guidelines published by the German Federal Office for Information Security ■ ID Documents conforming BSI TR-03127 eID application	■ Fujitsu PalmSecure truedentity enables scenarios of identity derivation from a primary identity (e.g. from an existing active directory account) ■ Fujitsu PalmSecure truedentity meets the official security requirements for authentication technology

Topic

Fujitsu PalmSecure truedentity technology stack

truedentity is a product family and consists of a technology stack, which contains both client and server components for the secure creation and handling of personal electronic identities. The truedentity clients offer one or more authentication methods, which differ both in terms of handling as well as the number of authentication factors. As a result, they map different security levels.
There is a relationship of trust between the truedentity client, truedentity server and eID-Server. While only truedentity client and eID-Server access the electronic ID during authentication, the truedentity server enables associating additional data to this ID. As part of an identity provider the eID-Server securely transmits the authentic identity information to the authorized service provider or target application that requires the identity information. Within the truedentity infrastructure is based on protocols used in the world of official documents.

User-centric authentication mechanism

truedentity is a user-centric authentication procedure. The eID-Server has the possibility of verifying the authenticity of the identity and enables the user to provide his authentic identification data to the service provider. Thus this server is the link between the user and the applications requesting the authentication. These applications are also referred to as identity consumers (IdC). The application range is large, from web applications that are connected via web technologies and standards such as SOAP (Simple Object Access Protocol) and SAML (Security Assertion Markup Language) up to and including integration with established identity protocols, such as Active Directory.

Comprehensible user authenticity

The truedentity authentication procedure uses PKI (Public Key Infrastructure) technologies with cryptographic methods. Electronic certificates maintain the authenticity of the communication and exchanged identities, while cryptographic methods safeguard this. The authenticity of the eID-Server is proven to the client. The procedures used ensure that identity data is only exchanged between trustworthy and authorized communication partners. The strength of truedentity lies not only in the provable authenticity of communication participants, but also especially in the flexibility of the truedentity client. The latter has the option of introducing new and additional authentication factors and of integrating them in various contexts. In this way, truedentity can be used in connection with a password if only a low protection level is required. In scenarios with higher security requirements, truedentity can also be enabled to provide stringent authentication factors, e.g. chip cards, biometric sensors. Other independent authentication mechanisms may be replaced with truedentity.

Great flexibility

The aim of the truedentity approach is not to integrate various existing authentication procedures and continue using them in a consolidated way, but rather to provide a flexible authentication interface. Depending on the given business case it is possible to vary the truedentity client and the authentication factors used (hardware token, biometric feature), while the communication technology and the truedentity ID used remain constant. The result of this is a variable range of web applications, which are connected by means of web technologies and standards such as SOAP (Simple Object Access Protocol) and SAML (Security Assertion Markup Language), right through to integration with established identity protocols, for example Active Directory. In addition to integration with the operating system, the usability of authentication in mobile applications is becoming more important.
The truedentity client is portable and deployable for different system architectures like ARM processors. An embedded truedentity client for the ID Match device is available, which enables authentication using the communication protocols offered by truedentity. In scenarios with high-security requirements, for example, truedentity can be combined with hardware components that have both a card reader and a PalmSecure palm vein scanner and thus enable multi-factor authentication in connection with biometrics.

Use of protocols for official documents

The Communication within the truedentity infrastructure is based on protocols used in the world of official documents. These include the PACE (Password Authenticated Connection Establishment) and EAC (Extended Access Control) protocols, which are internationally accepted and publicly documented in a Technical Guideline of the German Federal Office for Information Security (BSI). Among other standardized mechanisms these protocols are used for secure authentication with electronic ID documents and were examined with regard to their security features by independent research institutes. PalmSecure truedentity adapts this method and provides the option of integrating various authentication media. The use of standardized technologies and protocols also results in a high degree of compliance with changing legislation in the public sphere.

Technical Details

PalmSecure truedentity		
Server Components	truedentity Server (Registration Service, Personalization Service, Remote Storage, Administration)	
	eID-Server	
	Cryptoserver	
	PKI (EJBCA)	
	truedentity Integration Kit	
Clients	ID Match Authentication Client	
	Desktop Authentication Client (PalmSecure)	
	ID Match Personalization Client	
	Desktop Personalization Client	
Active Directory Bridge (optional)	Credential Providers for Windows Domain-Logon (with / without ID Medium)	
	Windows Authentication Service	
ID Documents	ID Documents conforming BSI TR-03127 eID application	
ID Mediums	Mifare classic	
	Mifare DESFire EV 1	
	HID ProxCard	

Minimum System Requirements (Server)		
Hardware	truedentity Server	CPU: Min. 2x Intel Xeon CPU (3.5GHZ, QuadCore), RAM: 8GB, HDD: Min. 50GB
	eID-Server	CPU: Min. 2x Intel Xeon CPU (3.5GHZ, QuadCore), RAM: 8GB, HDD: Min. 50GB
	eID-Server Front-end	CPU: Min. 2x Intel Xeon CPU (3.5GHZ, QuadCore), RAM: 4GB, HDD: Min. 50GB
	Cryptoserver	CPU: Min. 2x Intel Xeon CPU (3.5GHZ, QuadCore), RAM: 8GB, HDD: Min. 50GB
	PKI	CPU: Min. 2x Intel Xeon CPU (3.5GHZ, QuadCore), RAM: 8GB, HDD: Min. 50GB
Software	Operating Systems	Debian 7 & 8 (64-Bit)
	Runtime Environment	Oracle Java 6 & 8
	Application Servers	JBoss EAP 6.4, Glassfish 2.1.1
	Database	MYSQL

Minimum System Requirements (Clients)		
Hardware	Optional Peripherals	Fujitsu PalmSecure, Card Reader, ID Mediums (see above)
	Windows Clients	See operating system requirements
	ID Match Clients	ST (standard terminal)
		ID Medium support for Mifare classic & Mifare DESFire EV 1
Software	Windows Clients	Windows 7, 8.1 with current SP
	ID Match Clients	Linux based embedded operating system (standard terminal)

truedentity Integration Kit	
Software	Oracle Java 8

More information

Fujitsu products, solutions & services

Products
www.fujitsu.com/global/products/
In addition to the Fujitsu PalmSecure and PalmSecure truedentity Fujitsu offers a full portfolio of other computing products.

Computing products
- Storage systems: ETERNUS
- Servers: PRIMERGY, PRIMEQUEST, Fujitsu SPARC M10, BS2000/OSD Mainframe
- Client Computing Devices: LIFEBOOK, STYLISTIC, ESPRIMO, FUTRO, CELSIUS
- Peripherals: Fujitsu Displays, Accessories
- Software
- Network

Product Support Services with different service level agreements are recommended to safeguard each product and ensure smooth IT operation.

Solutions
www.fujitsu.com/global/solutions
The Fujitsu solutions combine reliable Fujitsu products with the best in services, know-how and worldwide partnerships. Fujitsu's solutions include parts of one or more activity groups (e.g. planning, implementation, support, management, and training services) and are designed to solve a specific business need.
Infrastructure Solutions are customer solutions created by bringing Fujitsu's best products, services and technologies together with those from partners to deliver benefit to our customers' businesses.
Industry Solutions are tailored to meet the needs of specific verticals.
Business and Technology Solutions provide a variety of technologies developed to tackle specific business issues such as security and sustainability, across many

Services
www.fujitsu.com/global/services/
Several customizable Fujitsu Service solutions ensure that IT makes a real difference and delivers true business value. We do this by leveraging our extensive experience in managing large, complex, transformational IT programs to help clients in planning, delivering and operating IT services in a challenging and changing business environment.

Application Services support the development, integration, testing, deployment and on-going management of both custom-developed and packaged applications. The services focus on delivering business and productivity improvements for organizations.
Business Services respond to the challenge of planning, delivering and operating IT in a complex and changing IT environment.
Managed Infrastructure Services enable customers to deliver the optimal IT environment to meet their needs – achieving high levels of IT service quality and performance for data center and end-user environments.

Fujitsu Green Policy Innovation

www.fujitsu.com/global/about/environment/
FUJITSU Green Policy Innovation is our worldwide project for reducing burdens on the environment. Using our global know-how, we aim to resolve issues of environmental energy efficiency through IT. Please find further information at:

Green Policy Innovation

More information

To learn more about Fujitsu, please contact your Fujitsu sales representative, Fujitsu business partner
or visit our website.
www.fujitsu.com/palmsecure/

Copyright

Disclaimer

Contact:
FUJITSU
Fujitsu Technology Solutions GmbH
Mies-van-der-Rohe-Strasse 8,
80807 München, Germany
E-Mail: palmsecure@ts.fujitsu.com
Website: www.fujitsu.com/palmsecure
2016-02-19