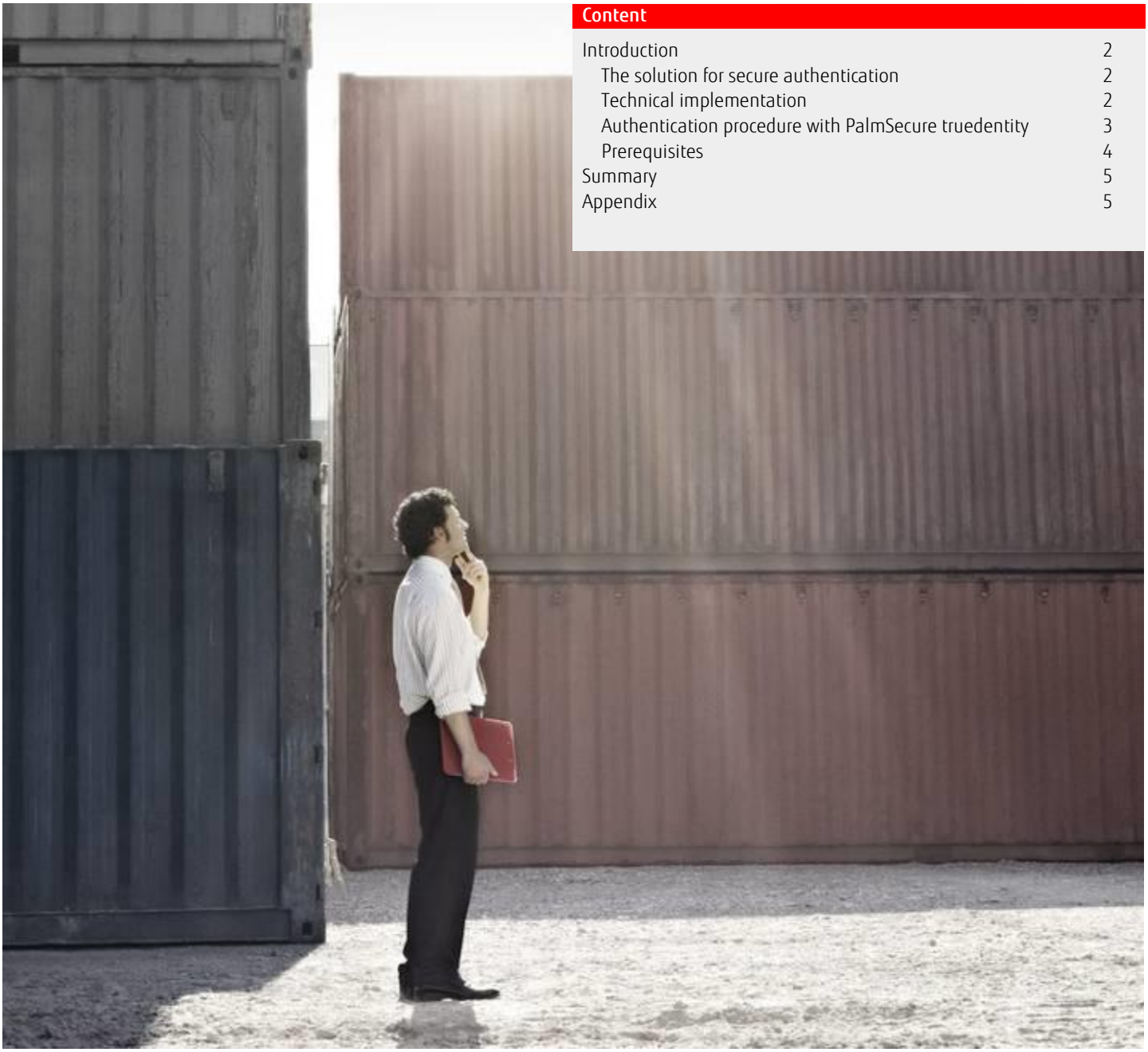
White Paper
PalmSecure™ truedentity®

Fujitsu PalmSecure truedentity is used for mutual service and user authentication. The user's identity always remains in the possession of the user. A truedentity server verifies the authenticity of the identities of both partners and permits access to the identity data.

Content



Introduction

Users wishing to access services generally have to prove their identity. This is either personally on-site (e.g. vehicle registration), or electronically by logging into or registering for a service. The identity of the user is entered with the respective data, i.e. the user must identify himself. The entered data can comprise name, address, date of birth, bank account number, etc. and is saved in the form of basic or user data.
If continued or regular access of services is required and the customer data has already been saved, the user is issued a "user account" and normally assigned a user name and password for authorization purposes. The customer can use this user name and password to prove his identity to the service. The user name and password are saved centrally in order to verify during authentication whether the user is authorized to access the services and protected information.

However, user names and passwords are weak identification features and can be easily copied, used by unauthorized persons, stolen and misused. Numerous solutions have been introduced in the past which have attempted to foil such a weakness, e.g. the introduction of organization measures (long, complicated password, frequent password changes) or technical measures using technology such as cards and chips), as well as additional features (dual or multi-factor authentication), such as PINs, TANs or biometric features. Today's technology is usually two-factor authentication with a chip card and PIN. However, cards too can be copied and the PIN can be accessed by unauthorized persons, e.g. when paying per credit card in a restaurant on holiday.

A basic vulnerability and risk always exists. Using the principle of user name and password or card and PIN, regardless of any improved technical and/or organization methods runs the risk of login data being intercepted after any non-authorized access to the central information stored on a database. There is also a danger that all user data can thus be intercepted and misused via a central attack on the user database. Repeated press stories have reported on such situations where service providers, such as web shops, social networks or other Internet platforms, have requested their users to change their passwords. Users can also be deceived and become victims when a "pseudo-service" masquerades as a regular service. The user has no simple method of verifying whether the service being accessed is actually the service it pertains to be. The user has no proof of authenticity for the service. Users generally assume that they are communicating with the correct partner based on an identical site appearance and an apparently correct address.

And this is exactly where PalmSecure truedentity technology takes over. It generates a person-related link between identity and enforces authentication of the service for the user. This document describes the range of services offered by PalmSecure truedentity technology.

The solution for secure authentication

PalmSecure truedentity is based on the technology used in the new German ID card and on the technical guidelines issued by the Federal Office for Security in Information Technology (BSI) and has been jointly developed in conjunction with OpenLimit SignCubes AG. In-depth development knowhow in the eID process sector, resulting from the development of the ID card app (AusweisApp) and an eID server for the new German ID card by OpenLimit SignCubes AG, ensures a flexible security concept that offers on-demand data protection based on the prerequisites of calculated investments.
The basic principle is that customer data no longer has to be stored with the service provider; it is scanned when required. An additional service, the so-called identity provider, is integrated in the communication with an intermediary role during joint authentication. It confirms to the user the correctness of the service identity and takes on the task of identifying the user for the service provider. An authorization certificate, registered by the identity provider and which must be applied for by the service provider, is the basis for authentication. The identity data of the user is stored securely and locally on a chip card. The user decides during authentication whether he releases the data or refuses the data. The identity data is transmitted using special, highly-secure transfer procedures.

The personal palm vein geometry of the owner is also saved as an additional biometric feature in order to protect the user's identity if the card is lost, stolen or copied. The palm-vein geometry is compared with that of the user before issuing the identity data (1:1 comparison). This ensures that the card user really is the owner of the card and is thus authorized to release the ID data to the service requesting the data. Any misuse through stolen cards is detected and prevented in advance..

The advantage of biometric procedures is that they are linked to only one person. Compared to other biometric procedures, the advantage of Fujitsu's biometric palm vein detection is that it is very secure. The palm vein pattern is invisible in the hand. A scan only functions when blood flows (live recognition). The pattern with its more than 5 million reference points is extremely complex and therefore 100 times more exact than, for example, fingerprint identification. The solution also runs on mobile terminals and can be optimally adapted to IT infrastructure and user behavior.

Technical implementation

The truedentity ID is not a sovereign ID document, but an electronic identity which can be used as a service ID card or for physical access control. This technology replaces silo architectures. Identities are no longer managed in a large number of databases. The user has his identity with him locally and can provide proof of identity at a central location when required to do so.

To put it simply, the system functions as follows: PalmSecure truedentity has the same access restrictions for identity data access as those with the new personal ID card (nPA). This means that firstly the user must agree to the access procedure for personal data and secondly the

participating service provider must prove his identity to the truedentity server via a certificate. This mechanism of mutual authentication between user and service provider is the same as the new personal ID card (nPA). This also verifies the card owner based on his/her biometric features, i.e. palm vein geometry. The data transfer is via specially secure and separate communication channels and procedures.

The truedentity authentication procedure is based on PKI (Public Key Infrastructure) with cryptographic procedures. Electronic certificates safeguard the authenticity of the communication and exchanged identity data whereas cryptographic procedures implement confidentiality and counterfeit protection. The authenticity of the truedentity server is ensured for the client and the associated procedures ensure that identity data is only exchanged with trustworthy and authorized communication partners. The implemented procedure is based on the EAC protocol. This protocol is used for secure authentication with electronic identity documents and its security features have been tested by independent research institutes. truedentity adapts this procedure and provides an option of integrating various authentication media.

Three parties communicate in a single authentication procedure with PalmSecure truedentity :

- An Identity Consumer (IdC) (service provider) is a service or program which scans an electronic identity and issues authorizations based on the identity information received, e.g. it permits access to an otherwise unavailable web page.
- The client is a program that has the electronic identity and which makes it available to a consumer on request.
- The Identity Provider (IdP) is a service, which is required to create an electronic identity; it is later required for access and to confirm the authenticity of the electronic identity.

The identity consumer and the identity provider must trust each other. This means that an electronic identity, created and confirmed by an identity provider, will be processed by the identity consumer. The identity consumer trusts the authenticity of the electronic identity which has been created and confirmed by the identity provider. When an electronic identity (truedentity ID) is created for a user, it is signed with a personal certificate (X.509). When logging on to a service provider, the latter can check whether the truedentity ID is genuine and valid, and can then forward the inquiry to the identity provider. Via OCSP (Online Certificate Status Protocol) and blacklists, the identity provider can determine whether the truedentity ID is valid or has been disabled for any particular reason. When creating a user's truedentity ID, the palm vein geometry is scanned via Fujitsu PalmSecure and saved on the card locally. This feature remains constant for a person's lifetime and is even different for identical twins. The card can thus not be used by someone else.

Identity technology provides various deployment areas. They are always scenarios in the Internet, for example, authentication in a payment procedure (POS) or registering with a web-based system or cloud storage. The solution provides the following advantages:

- The solution is a proven method: the client and server technologies provided by OpenLimit SignCubes AG have been completely redeveloped in Germany and made more professional as part of the new ID card development process. OpenLimit SignCubes AG technologies for handling electronic identities is implemented, for example, by the Bundesdruckerei GmbH, DATEV, Fraunhofer Fokus.
- The solution is flexible and this approach has a large number of different scenarios.
- The technology is secure: The implemented technical procedures are state-of-the-art technology. The communication procedures used are compatible with the technical guidelines, used as a basis for the online authentication technology in the new German ID card is based.

Authentication procedure with PalmSecure truedentity

In order to gain access to a user's data, the service provider must authenticate itself in each transaction, just like the user. The authorization certificate defines the identity data which the service provider may scan. The data is then released via the biometric identity. It can also entirely reject access.
The details of the authentication procedure with truedentity are as follows:

1. The user clicks "Login" on the service provider side
2. The truedentity server is now requested by the service provider and the client to authenticate the respective parties.
3. The service provider data is valid
4. The user identity signature is valid
5. The data requested by the provider is displayed (according to the service provider's authorization certificate). This can also be optional.
6. The user is requested to release the identity data via palm vein validation
7. The identity data is then transferred to the provider
8. The user is logged on to the provider service

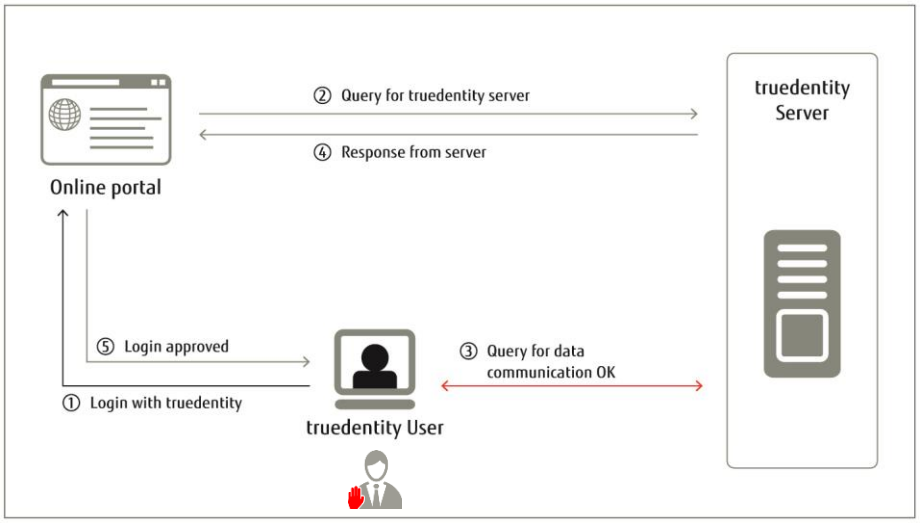


Figure 1 - Authentication procedure with truedentity

Each communication between the browser, truedentity client, web server and truedentity server is TLS encrypted. The transferred data is also encrypted. Communication between the truedentity client and the truedentity server is based on protocols used in the world of sovereignty documents.

A truedentity client is required to ensure secure authentication and to create the electronic identity (personalization). The truedentity server is the link between the truedentity client and the web site, i.e. between the end user and the service provider. It is the trust instance in an authentication process using truedentity client via the Internet. The truedentity server checks whether the service provider is authorized to scan the truedentity identity data and whether the truedentity identity is genuine or whether it has been reported as stolen. In order to handle personal data confidentially during the transfer, the truedentity server encrypts and signs the data. The truedentity server is designed as a logical separate server so that it can be used by several web applications. It is client-compatible and can be leased as a service.

The issue of identities is implemented via the identity provider with the registration and personalization service. An activation code must be entered in order to create a user identity. The former is generated via the registration service.

In order to create the identity, the activation code is scanned by the personalization service in conjunction with the truedentity client. After its input and verification, the end-user is then requested to set a password. The identity is then saved in the truedentity client or on a smartcard. Tailor-made PK infrastructures are used to create secure identities, for secure transfer in public networks and for the secure identification of authorized services. PKI stands for Public Key Infrastructure; it denotes secure communication and identification using private and public keys.

In some countries e.g. Germany it's not allowed to store biometric signs or templates centrally. Palmsecure truedentity offers both possibilities: to store the biometric template on a card or central on a host system. Solutions can be tailored to the customers' requirements. It's also possible to build a card less solution, identifying only by scanning the vein pattern at the device.

Prerequisites
The following list identifies the operational environment for each component.

truedentity server
- Hardware requirements:
  Front-end: CPU: Min. 2x Intel Xeon CPU (3.5GHZ, QuadCore), RAM: 16GB, HDD: Min. 500GB
  Core application: CPU: Min. 2x Intel Xeon CPU (3.5GHZ, QuadCore), RAM: 32GB, HDD: Min. 500GB
  Back-end: CPU: Min. 2x Intel Xeon CPU (3.5GHZ, QuadCore), RAM: 32GB, HDD: Min. 500GB
- Software requirements:
  Respectively: Linux 64-Bit (RedHat, Debian, openSUSE etc.), Oracle Java 8
  Application server: JBoss-based

truedentity Client:
- Operating system: Windows 7, 8, 8.1 with current SP and drivers for PalmSecure
- Chipcards: E4 NetKey with TCOS 2.0 Chip OS, TCOS 3 cards (other chipcards can be integrated on request).
- Fujitsu PalmSecure ID Match Device as card reader and palm vein scanner

Summary

Fujitsu PalmSecure truedentity is used for mutual service and user authentication. The identity of the user remains the user's property. A truedentity server verifies the authenticity of both partners' identities and permits access to identity data. The application range varies between web applications that are linked 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.

The strength of PalmSecure truedentity lies not only in its forgery protection and proof of authentication for the users, but also in the flexibility of the truedentity client. This can be used to introduce new and extra authentication factors. Truedentity can be used as a substitute to authentication with a user's name and password if only a low protection level is required. In scenarios with higher security requirements, truedentity can also provide stringent authentication factors, e.g. chipcards, biometric palm vein detection or implemented additional independent authentication channels, such as a TAN procedure.

This approach enables the use of parallel scenarios to derive an identity from a primary identity, as well as a migration option for electronic identities. Identity derivation is the process of issuing an electronic identity based on a primary identity. A primary identity can be an official identity document – e.g. a new state ID card. This information is the basis for a process to create a derived identity and for its use in authentication scenarios. This approach avoids the use of a static, externally specified authentication medium, such as a new ID card, the use of which in a commercial environment is subject to legal restrictions.

Appendix

Links: https://www.openlimit.com/en/products/truedentity.html

Contact
FUJITSU
Phone: +44 (0) 870 242 7998
E-Mail: cic@ts.fujitsu.com
Website: www.fujitsu.com/palmsecure
2015-05-24