
Fujitsu
World Tour
2015
Security as an Important
Contributor to Business Success
FUJITSU
shaping tomorrow with you
Human Centric
Innovation

A Hyperconnected World

FUJITSU

- An emerging new world where people, information, things and infrastructure are connected via networks, transforming work and life everywhere
- Data is the most important part of ICT and has the highest value
- Information is leaving secured data centers

Internet of Things & Big Data

FUJITSU

- IoT & big data bring huge growth potential to the global economy
- We also face serious challenges of security and privacy

Things connected to the internet

2013 10 billion
2020 50+ billion

3.6 TB/h - A self-driving car
20T B/h - A jet engine in the air
100 GB - An individual genome

The workplace environment is changing

- Past: Working in secured buildings with dedicated workplaces and set times
- Today & Future: Working at your own terms, anywhere, at any time

What does it mean and what is the impact ?

FUJITSU

- (Critical) data are leaving companies
  - The data center is mostly a mobile device
- Poor protection versus data centers
  - Mostly only an (un)actual virus scanner is standard
- Data become values and are handled for money, e.g.
  - Social data
  - Accounts with password
  - Credit data
- Data are easily available

- In Pbyte more data are available outside as inside a company – „big-data-mobility“
- Data centers are highly protected e.g. access, monitoring, damage, data loss
- Dealing of data earns more money as with IT equipment e.g.
  - Social Networks
  - E-Commerce
  - Finance / Retail Services
- Every organization deals with huge data volume

Definition of IT Security

FUJITSU

:: **CONFIDENTIALITY** ::

Confidential information has to be protected against unauthorized distribution & usage

:: **AVAILABILITY** ::

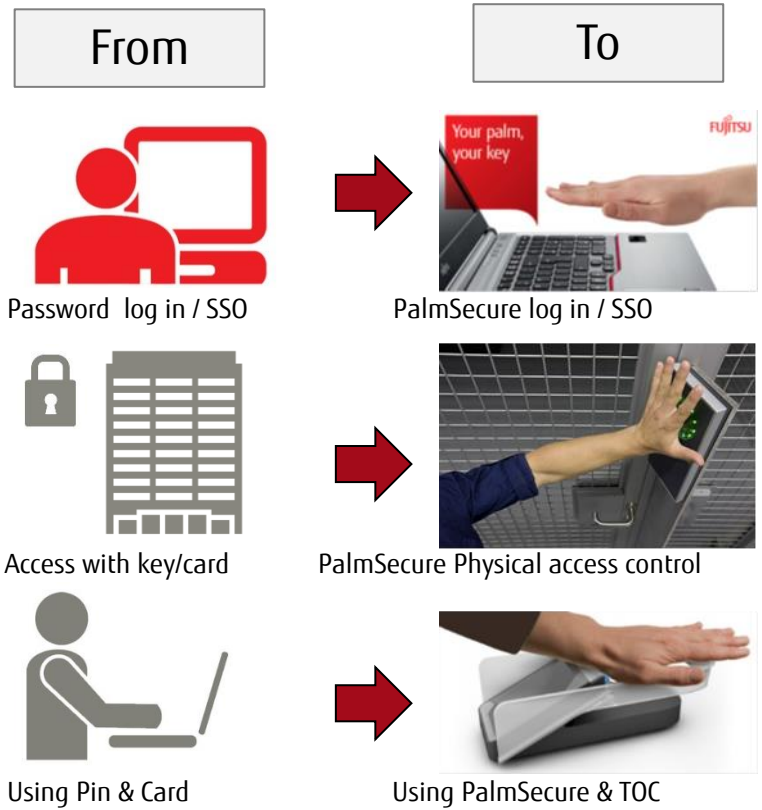
The user must have access to IT services, to IT information and to functions of the IT system at any time

:: **INTEGRITY** ::

All data has to be provided in full and unaltered

Solving today´s IAM topics with PalmSecure based solutions

- **Current situation:**
  - Increased ID frauds globally
- **Customer pain points:**
  - Stolen & misused personal identities causing slower processes & increased costs & causing non satisfied customers & employees
- **This will happen in the market:**
  - Investing in high secured "easy to handle" professional IAM solutions / services
- **What Fujitsu is offering:**
  End to End security solutions & services based on Palm Vein biometric authentication technology



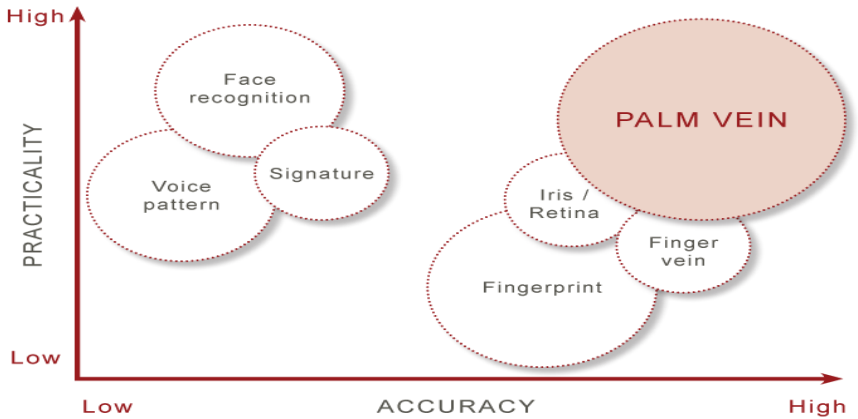
PalmSecure IAM areas

Ca. 200 Million Users Globally!

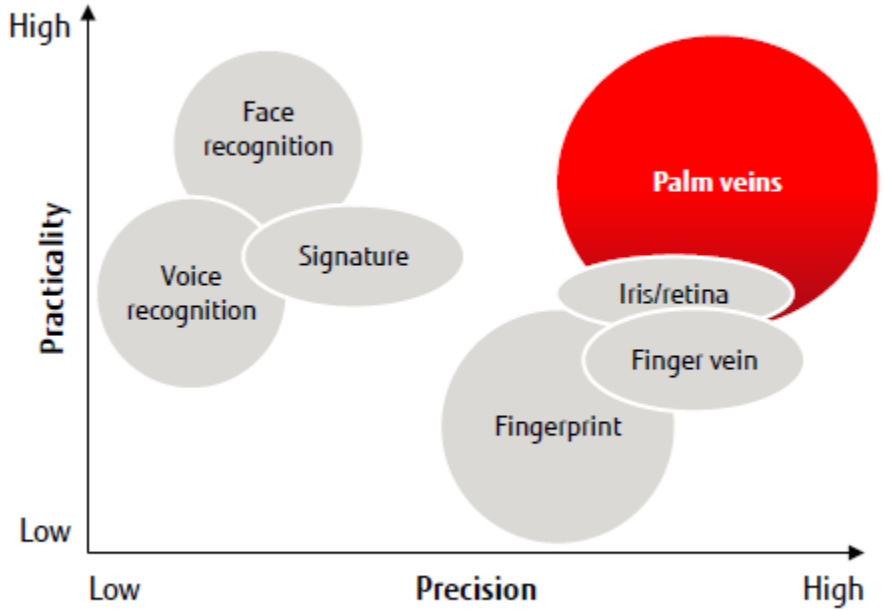
Workplace Protect

- Single application for all security relevant settings
- Protects workplace devices against unauthorized usage
- Automatically locks workplace devices, when user leaves his/her desk
- Supports a wide range of security devices
- Comes pre-installed on Fujitsu Client Computing Devices
- Free of charge for Fujitsu Client Computing Devices

Authentication Method	FAR (%) =	If FRR (%) =
Face recognition	~ 1.3	~ 2.6
Voice pattern	~ 0.01	~ 0.3
Fingerprint	~ 0.001	~ 0.1
Finger vein	~ 0.0001	~ 0.01
Iris/Retina	~ 0.0001	~ 0.01
Fujitsu Palm vein	**< 0.00008**	~ 0.01



USPs of PalmSecure Technology



- Not able to copy → pattern is under the skin
- Alive detection
- Long-lasting → structure never changes
- Precise → measuring > 5 Mio ref. points
- Touchless → hygienic
- "Robust" → thick veins

PalmSecure ID Match

- Cutting Edge Technology
- Ultimate Convenience
- Maximum Security
- Independent Functionality
- Stylish, Hygienic Design
- Prepared for Multiple Applications

PalmSecure ID Match - Advantage

No personal biometric data is stored on a server or in the cloud.

The "**matching**" of the template on the card and user's hand are **done in the device**.

Misuse in a positive (give your card and PIN away) or negative way (stolen card and or PIN) **is eliminated by this technology**.

Legal perspective data protection biometric

FUJITSU

Laws governing data protection and data security e.g.:

- Acquisition, storage and processing of biometric data is only permitted if either a **legal basis** or **a voluntary and informed consent from the person involved** is available
- According to the principle of appropriation, biometric data **may only be used for the purpose, for which they were collected**, for example for access control.

Requirements for the data protection agreement:

- Don't use raw data – use reference data (**templates**)
- Provide a choice of procedures
- **No central storage** for templates, but preferably somewhere in the exclusive control of the user (for example a SmartCard)
- Protection of biometric data from unauthorized access
- Use of **encryption**
- Transparency of procedures and security mechanisms

Conclusion:

Data protection problems do not apply if

- a central storage medium is not in use and
- the users manage the storage of their biometric characteristics themselves, such as a SmartCard
- EU requirement of 2 factor authentication for payment processes

Fujitsu PalmSecure ID Match is the perfect answer for legal requirements

PalmSecure Ultrabook U904

Hardware

- World's first notebooks with integrated sensor
  - FUJITSU Notebook LIFEBOOK U904 Ultrabook™
  - FUJITSU Workstation CELSIUS H730
- PalmSecure Mouse Login Kit and PalmSecure Sensor Guide Kit

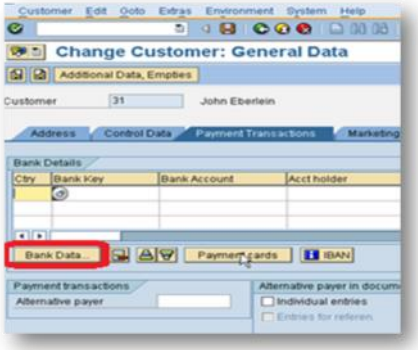
Software

Security made easy with Fujitsu's software solutions

- Workplace Protect
  - Supporting configuration of windows authentication, pre-boot authentication, single-sign-on, password safe and encrypted container
- Workplace Manager
  - Administrator console for remote management of security settings

PalmSecure bioLock for SAP

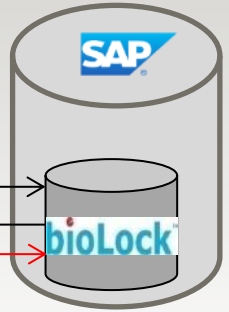
- Fraud prevention
- Data control
- Process logging
- Individually secured processes
- Controlled authorized financial transactions



User requests SAP activity.
e.g. Log-on, **SE16** data Browser, Customer Service activity

bioLock prompts user for biometric scan

Sample biometric template extracted, encrypted, compared with **reference** template in bioLock/SAP



Action Allowed

Action Denied

Activity logged

Current Date	bioLK User	Text	Text
19.06.2013	MILLER	was rejected	SAP Logon
19.06.2013	JONES	was accepted	SAP Logon
19.06.2013	SMITH	was accepted	SAP Logon

Innovative Palm Vein Authentication Advantages

FUJITSU

High Safety & Permanence

- Hidden under the skin - forgery difficult
- Unique even among identical twins
- Never change - same throughout life
- Detectable only when blood is flowing

High Accuracy

- Palm vein patterns are highly complex
- High applicability
- Designed for public usage
- Palm veins are insensitive against environment (cold temperature, creamy hands, skin scratches)

High Acceptance

- Very hygienic due to no-contact operation
- Very easy and intuitive to use
- Biometric pattern hidden inside the body (privacy)

FUJITSU

Thank you for listening!

Privacy e lavoro, il nuovo vademecum del Garante – Aprile 2015

- Il Garante della Privacy ha fornito indicazioni in relazione al trattamento dei dati personali dei dipendenti in azienda riassumendoli nel **vademecum** “**Privacy e lavoro”.**

- La guida sintetica si propone di illustrare con un linguaggio semplice e immediato il complesso tema della privacy sul posto di lavoro sia in ambiente pubblico sia privato, materia che spesso genera contenziosi tra dipendenti e datori di lavoro.

- Il vademecum è suddiviso in dieci sezioni: principi generali, cartellini identificativi; comunicazioni; bacheche aziendali, pubblicazioni di dati del lavoratore sui siti web e sulle reti interne; dati sanitari; **dati biometrici**; uso di internet/intranet e della posta elettronica aziendale (i controlli, Internet/rete interna, posta elettronica aziendale); controllo a distanza dei lavoratori (videosorveglianza e geolocalizzazione); documenti di riferimento.

- Il vademecum riporta anche i riferimenti alle linee guida e ai principali provvedimenti dell’Autorità in tema di trattamento dei dati dei lavoratori e può essere scaricato in formato digitale dal sito dell’Autorità.

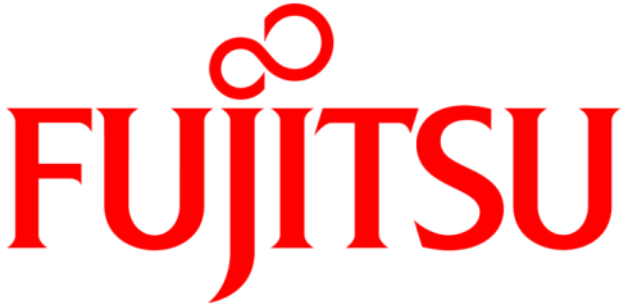
Adobe Acrobat Document

Dati Biometrici

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

FUJITSU

- Non è lecito l'uso generalizzato e incontrollato dei cosiddetti "dati biometrici" (quelli ricavati ad esempio dalle **impronte digitali** o dalla **topografia della mano**). Questi particolari trattamenti sono stati **esaminati dal Garante in un apposito provvedimento generale** (doc web n. 3556992 e doc web n. 3563006) **in cui sono state previste anche alcune ipotesi di esonero dall'obbligo della verifica preliminare del Garante**.
- **Le impronte digitali o della topografia della mano**, ad esempio, **possono essere usate** per presidiare gli accessi ad "aree sensibili" (processi produttivi pericolosi, locali destinati a custodia di beni di particolare valore e/o alla conservazione di documenti riservati) oppure per consentire l'utilizzo di apparati e macchinari pericolosi ai soli soggetti qualificati; l'impronta digitale o l'emissione vocale possono essere utilizzate per l'autenticazione informatica (accesso a banche dati o a pc aziendali); la firma grafometrica per la sottoscrizione di documenti informatici. Ciò nel rispetto, in particolare, di rigorose misure di sicurezza specificamente dettagliate nel provvedimento. **In alcuni casi individuati dal Garante, nel rigoroso rispetto delle cautele individuate, il datore di lavoro non è tenuto a richiedere il consenso al personale per adottare tecnologie biometriche, ma deve comunque informare i dipendenti sui loro diritti, sugli scopi e le modalità del trattamento dei loro dati biometrici.**
- **Non è generalmente ammessa la costituzione di banche dati centralizzate ma è preferibile l'utilizzo di altre forme di memorizzazione dei dati, ad esempio in smart card ad uso esclusivo del dipendente**. Nel caso in cui la tecnologia biometrica che si vorrebbe adottare non rientri tra i casi semplificati dal Garante, permane l'obbligo per il datore di lavoro di richiedere un'apposita verifica preliminare prima di iniziare il trattamento dei dati.



shaping tomorrow with you