
ORACLE®

ORACLE

Performante Verschlüsselung mit Oracle Hardware und Solaris

Stefan Hinker
EMEA Hardware Principal Sales Consultant

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions.
The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

Ntraqn

- Jnehz Irefpuyüffrya?
- Uneqjnerirefpuyüffryhat orv Benpyr
- Fbynevf Pelcgbtencuvp Senzrjbex
- Orvfcvryr

Agenda

- Warum Verschlüsseln?
- Hardwareverschlüsselung bei Oracle
- Solaris Cryptographic Framework
- Beispiele

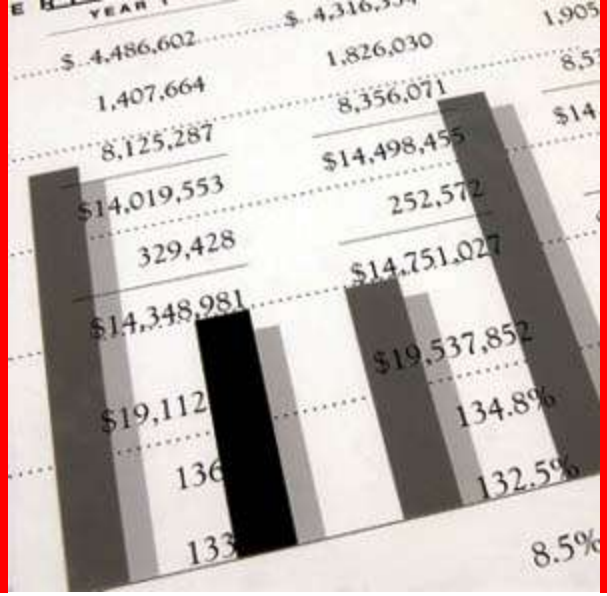
Warum brauchen wir Verschlüsselung?

- Kosten von Datenlecks können enorm sein
  - Laut Ponemon Institut* ca. $ 6.75 Millionen pro Fall
  - 40% der Vorfälle durch Nachlässigkeit
    - bspw. verlorener Laptop
- Teilweise gesetzlich vorgeschrieben
  - Bundesdatenschutzgesetz:
    - § 9 Technische und organisatorische Maßnahmen
    - § 42a Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten
- Unverzichtbarer Teil eines Sicherheitskonzepts

* http://pc.de/software/datenlecks-verursachen-kosten-397

Wo Verschlüsseln?

- Überall!
- Daten in Ruhe
  - Jede Festplatte & jedes Band verlassen irgendwann das RZ
- Daten Unterwegs
  - Schutz auch gegen Angriffe via Netzwerk
  - Damit snoop und tcpdump keinen Spass machen
- Daten bei der Verarbeitung
  - Nur benötigte Daten im Klartext
  - Heute noch wenig verbreitet
  - Beispiel: SCA 6000 – Klartext nur auf der Karte



ComputerWorld,
February 10, 2009

"A New York computer forensics company recently reported that 40% of the hard disk drives that it recently bought in bulk orders on eBay contained personal, private and sensitive information. "

(Sehr) Kurze Geschichte der Kryptographie

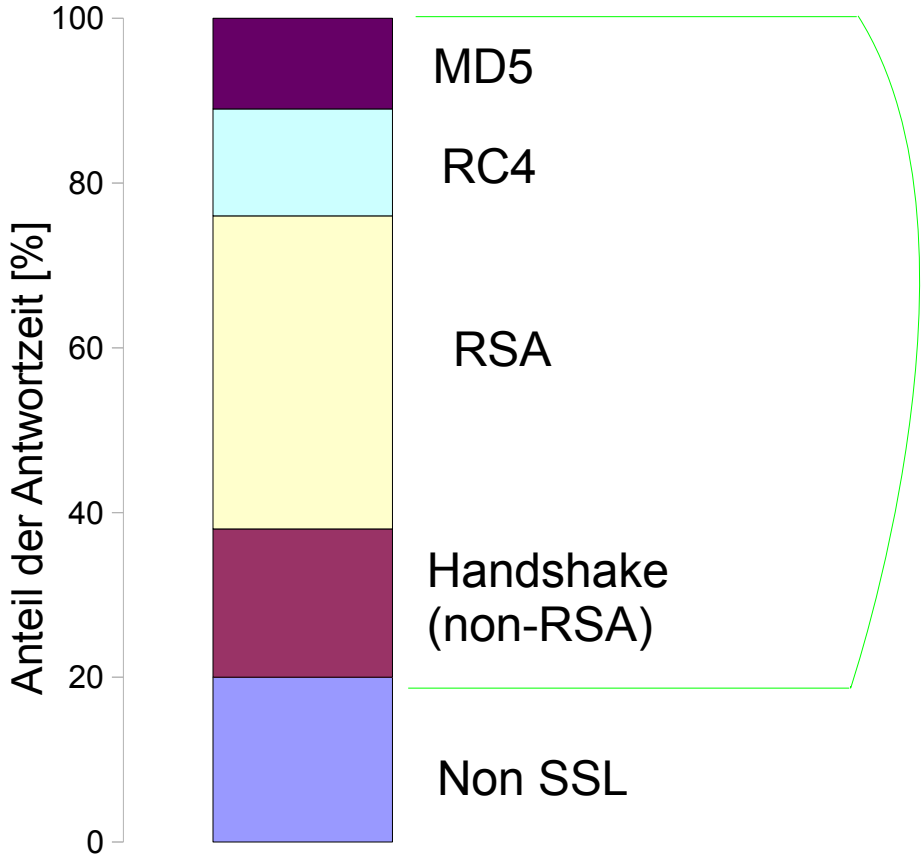
- Erste Verwendung ca. 1900 v. Chr. in Ägypten
- Caesar Chiffre ca. 100 v. Chr.
  - Variante heute noch als ROT13 bekannt
  - Erweiterung mit Schlüsselwort zur Vigenère Chiffre um 1553
- Enigma 1918
  - Mitverantwortlich für die Entwicklung der heutigen EDV
- Moderne Algorithmen
  - DES, AES für Vertraulichkeit
  - RSA, DSA, ECC für Authentifizierung

Verschlüsseln ist teuer

- Sichere Algorithmen bedeuten komplexe Mathematik
  - Damit einhergehende hohe CPU Last
  - Typisches Beispiel ist SSL Handshake
  - Abhilfe durch Hardware-Beschleunigung
- Schlüssel müssen verwaltet und sicher aufbewart werden
  - Standardisierung nach FIPS 140-2
- Nicht verschlüsseln ist noch teurer

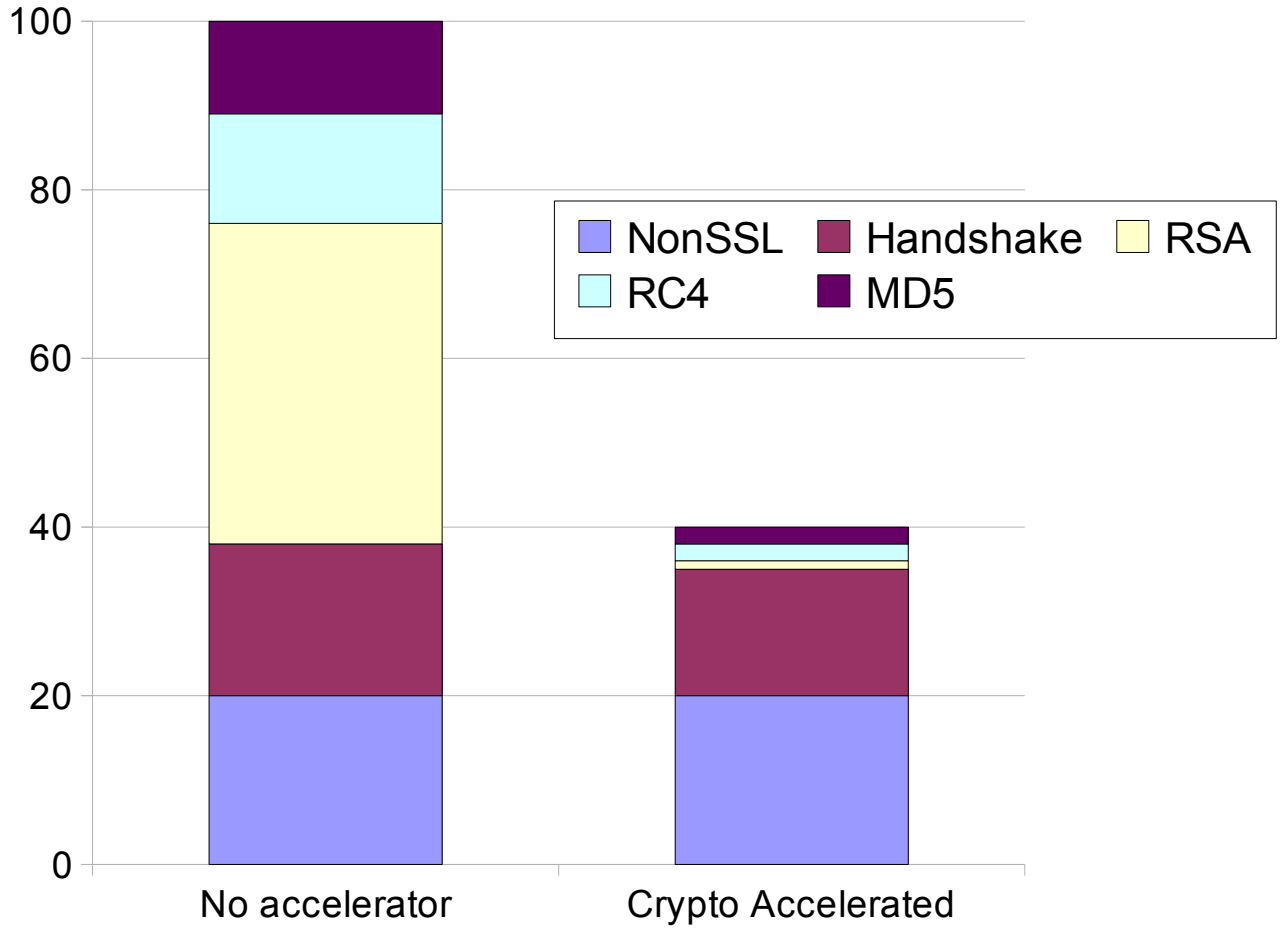
Warum Verschlüsseln so teuer ist: Beispiel SSL

Aus einer Studie von SPECweb2005



Fast 80% der Antwortzeit einer typischen SSL-Transaktion entfallen auf Crypto!

Gewinn durch Hardwarebeschleunigung



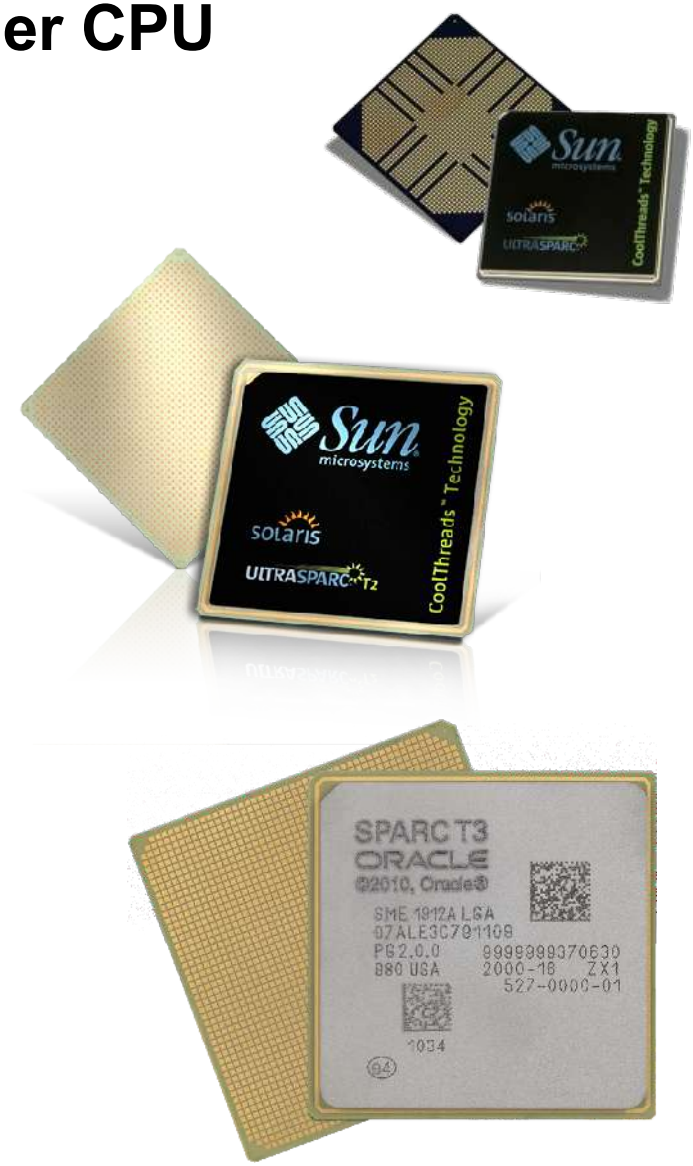
Agenda

- Warum Verschlüsseln?
- Hardwareverschlüsselung bei Oracle
- Solaris Cryptographic Framework
- Beispiele

Hardwarebeschleunigung in der CPU

SPARC T – Vielseitig und Schnell

- UltraSPARC T1 (2005)
  - Asymetrische Chiffren
    - SSL Handshake
  - RSA-1024: 12.000 Ops/sec
- UltraSPARC T2 (2007)
  - Zusätzlich Block Chiffren
  - RSA-1024: 41.000 Ops/sec
  - AES-128: 44 Gbit/sec
- SPARC T3 (2010)
  - 16 statt bisher 8 Einheiten
  - Modernisierte Algorithmen
  - RSA-1024: 79.000 Ops/sec



Hardwarebeschleunigung in der CPU

Intel Westmere EP (5600) – AES-NI

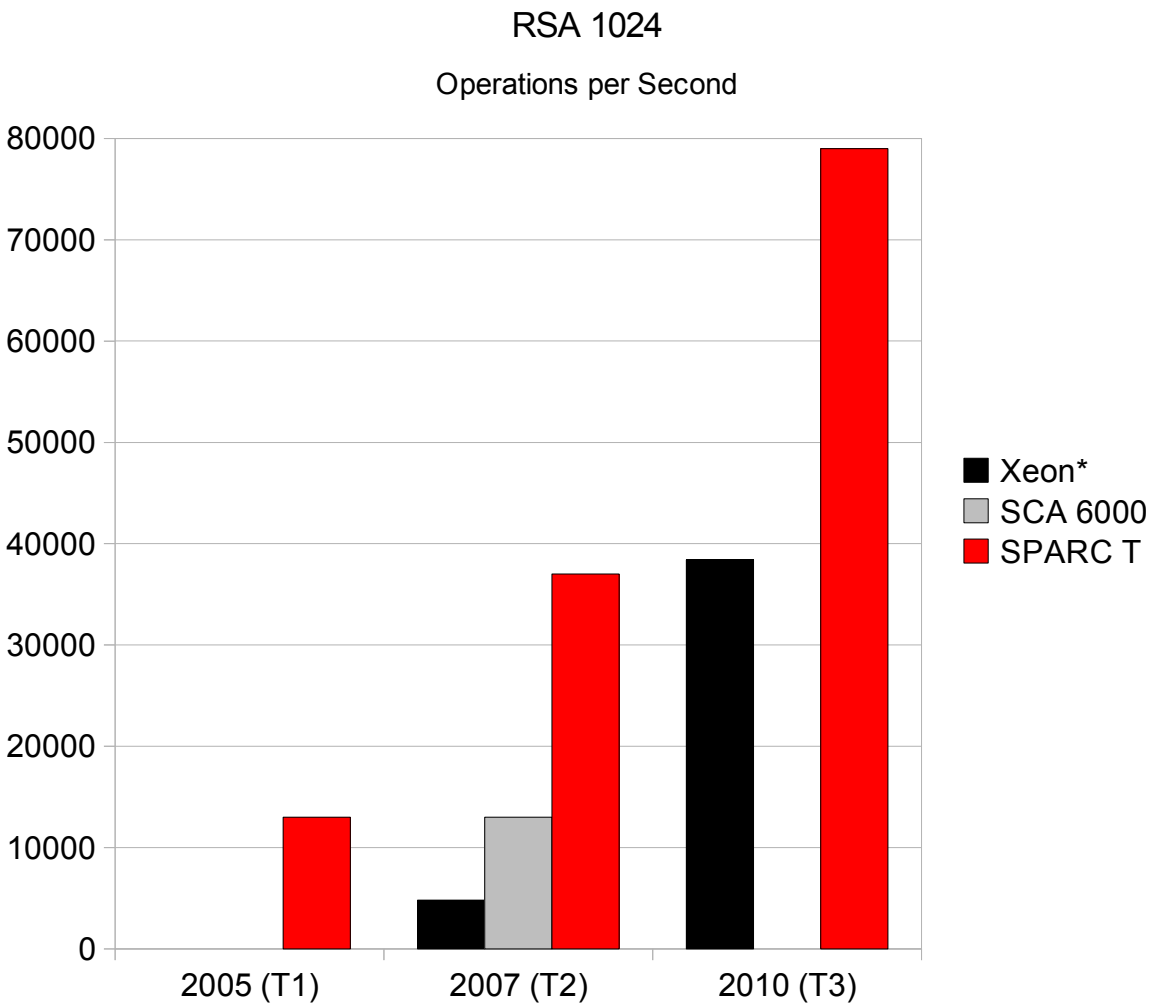
- Erste x86 CPU mit Crypto-Unterstützung
- AES-NI
  - 7 neue Instruktionen für AES
- Keine weiteren Chiffren
- Derzeit nicht virtualisierbar

Cryptographic Accelerator 6000

Beschleunigung & Sicherer Speicher

- Preiswerte PCIe-Karte
  - Treiber für Solaris und Linux
- Unterstützte Algorithmen
  - AES, DES, 3DES, RSA, DSA, DH, SHA-1 und MD5
- Kreditkarten-Unterstützung
  - PIN und Kartenverifizierung
- Sicherer Schlüssel-Speicher
- Zertifiziert nach FIPS 140-2 Level 3

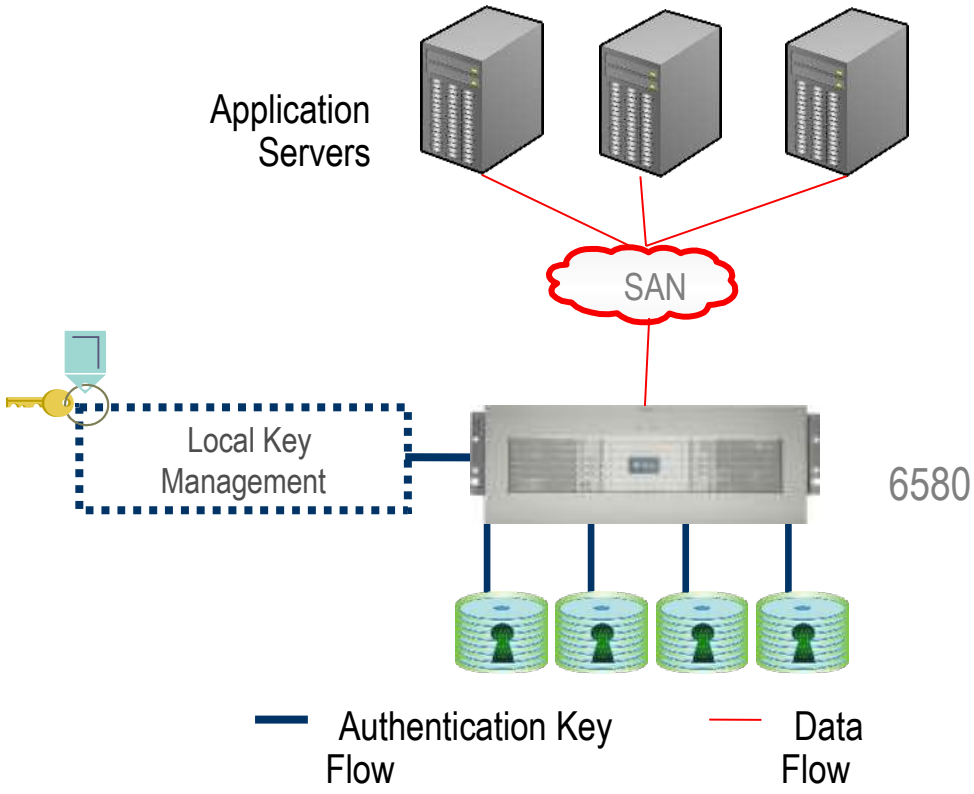
Performance von Hardware-Beschleunigung



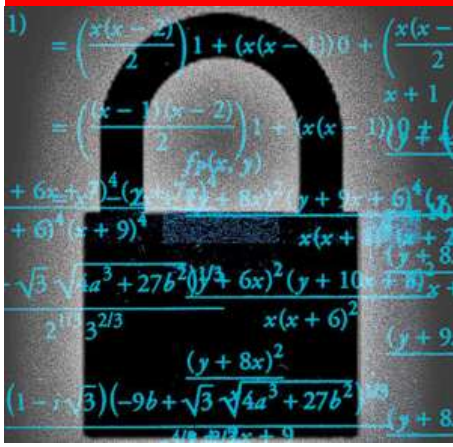
* Xeon 2010: Geschätzt 8x Xeon von 2007
Keine Vergleichbaren Daten bzgl. AES mit T3 oder Intel 5600 verfügbar. Siehe Referenzen.

Was es dann auch noch gibt

Data Encryption Services für die Storage 6000 Familie

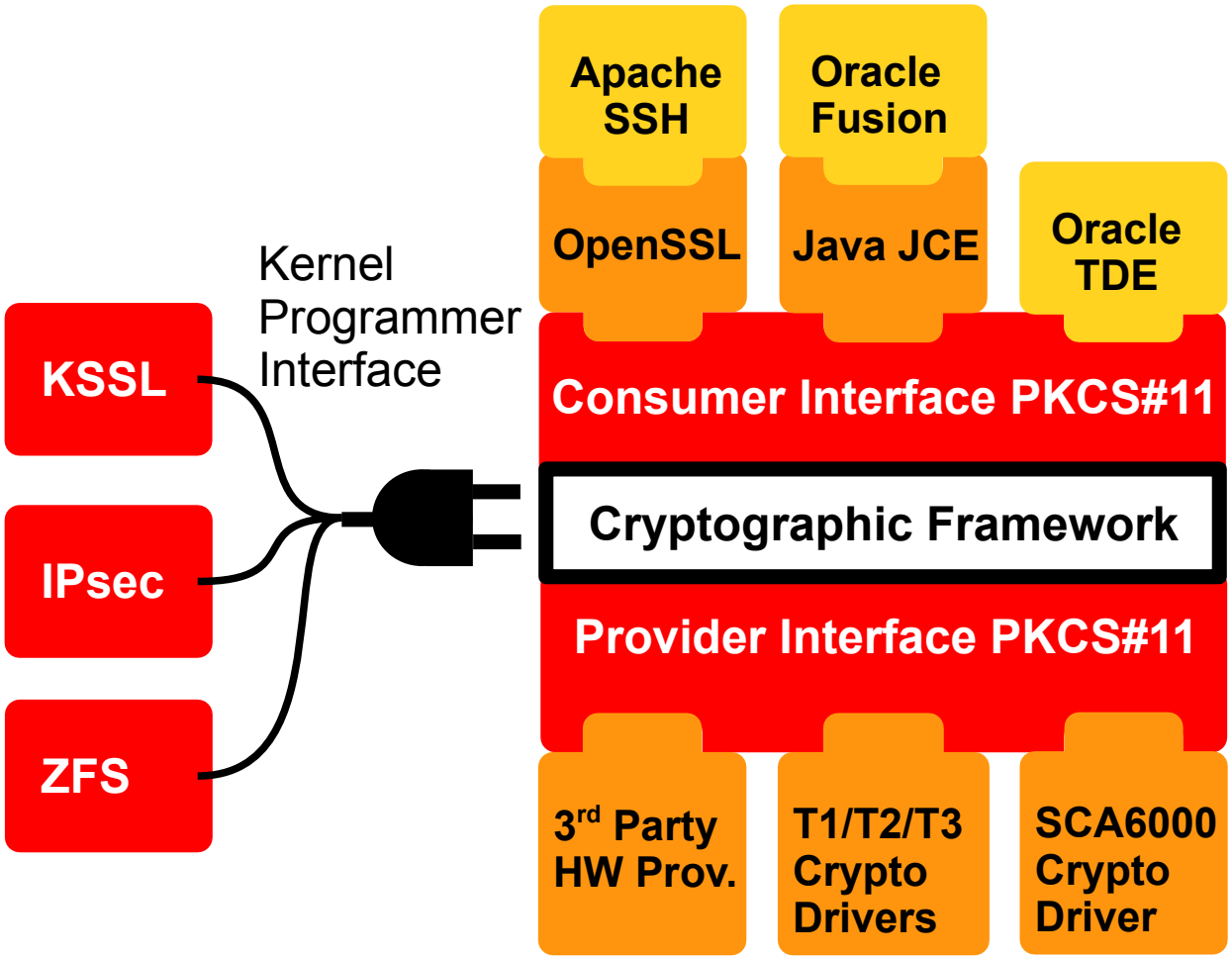


Agenda



- Warum verschlüsseln?
- Hardwareverschlüsselung bei Oracle
- Solaris Cryptographic Framework
- Beispiele

Das Solaris Cryptographic Framework



- cryptoadm
- pktool
- kcfd

Agenda

- Warum Verschlüsseln?
- Hardwareverschlüsselung bei Oracle
- Solaris Cryptographic Framework
- Beispiele
  - Apache
  - SSH
  - Java
  - Solaris KSSL Proxy
  - Oracle TDE

Beispiele – Apache

- Verwendet OpenSSL
  - PKCS#11 als Engine von OpenSSL
  - Korrekt konfigurierte Libraries in Solaris enthalten
  - ggf. Compiler-Option “-DSSL_ENGINE” verwenden
- SSL wie gewohnt konfigurieren
- PKCS#11 als Engine in der Apache-Konfiguration

```
SSLCryptoDevice pkcs11
```

Beispiele – SSH

- Verwendet OpenSSL
  - Integration jedoch komplex
- Seit Solaris 10 3/05 automatisch
- Konfiguration in /etc/ssh/sshd_config
- Vorteil insb. für scp und sftp
  - ca. 2x schneller auf UltraSPARC T2

```
UseOpenSSLEngine
```

Beispiele – Java

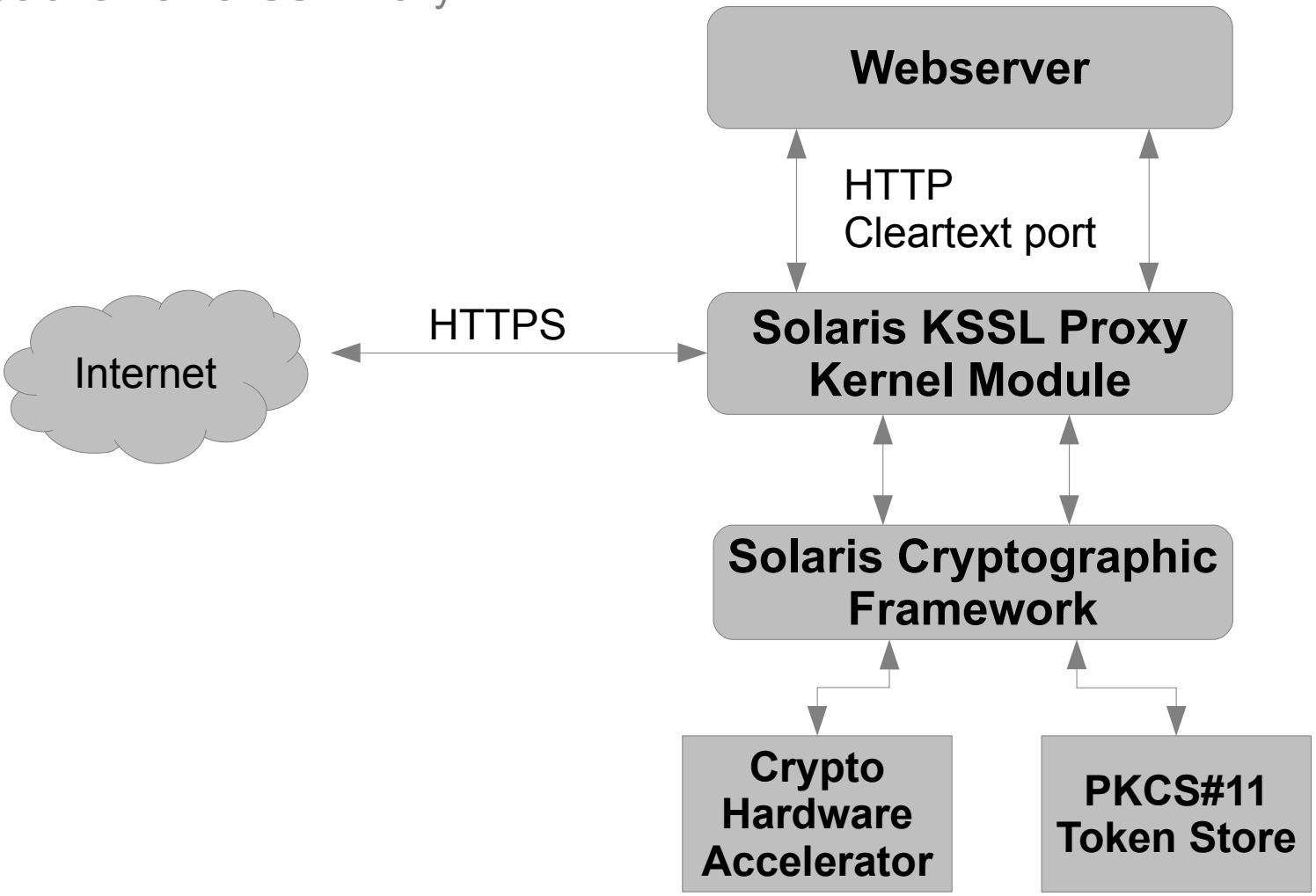
- Verschlüsselung als Teil der Java Cryptographic Extension (JCE)
- Fertig Klassen für verbreitete Chiffren
- Hardware-Unterstützung wird automatisch genutzt
- Konfiguration in $JAVA_HOME/jre/lib/security/java.security

```
security.provider.1=sun.security.pkcs11.SunPKCS11
```

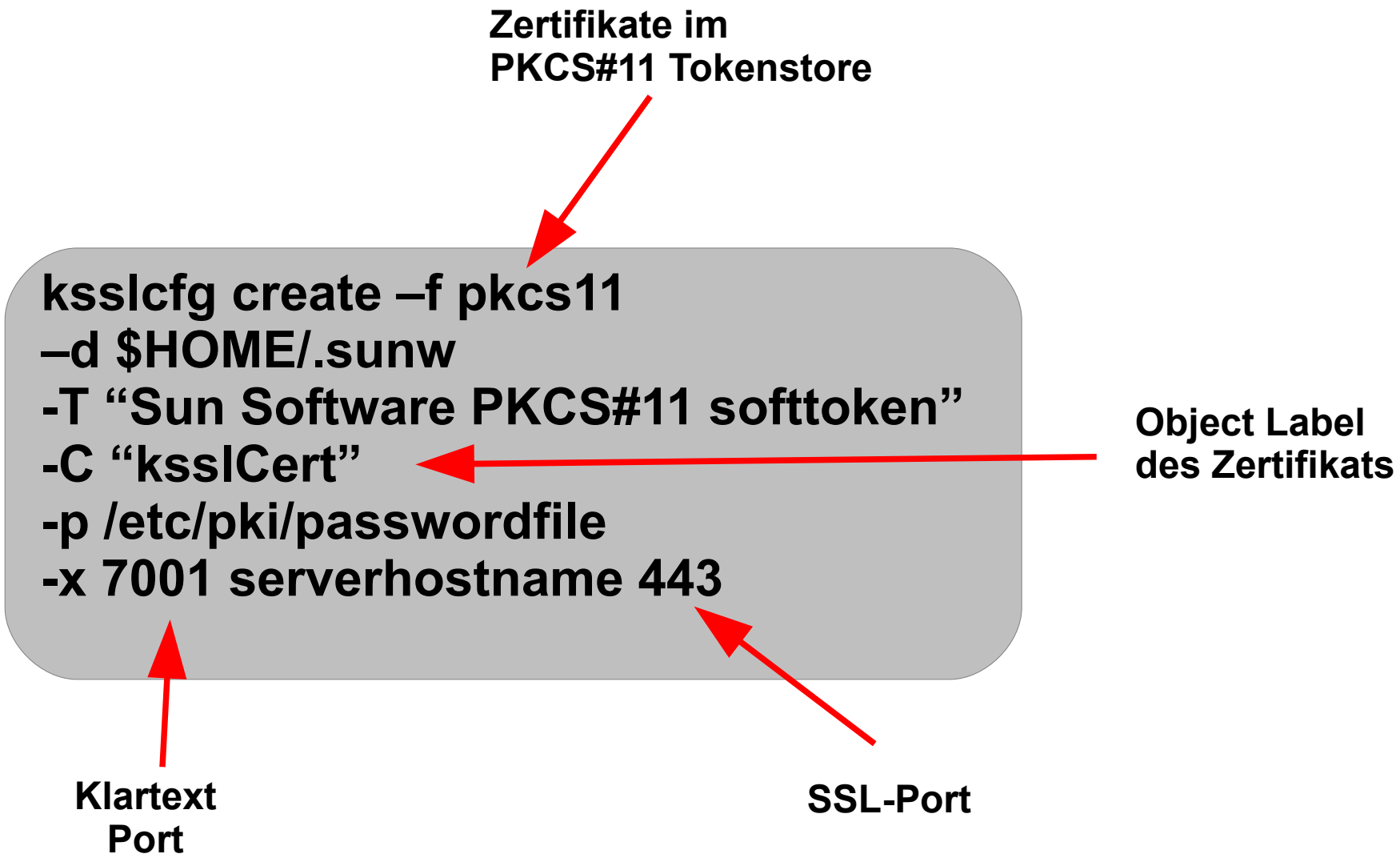
- Ggf. weitere Mechanismen freischalten in sunpkcs11-solaris.cfg

Beispiele – KSSL

Solaris Kernel SSL Proxy

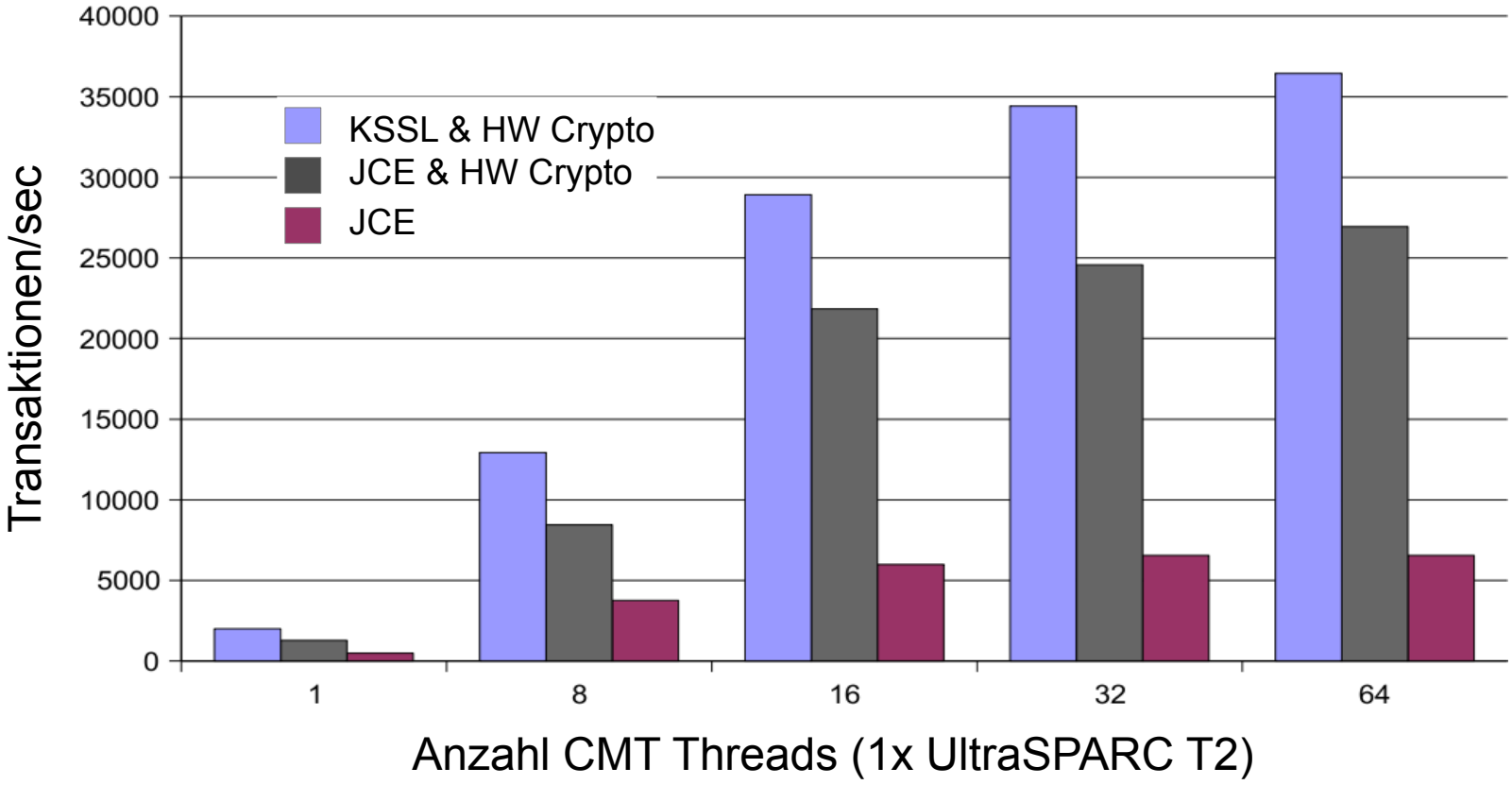


KSSL – So geht's



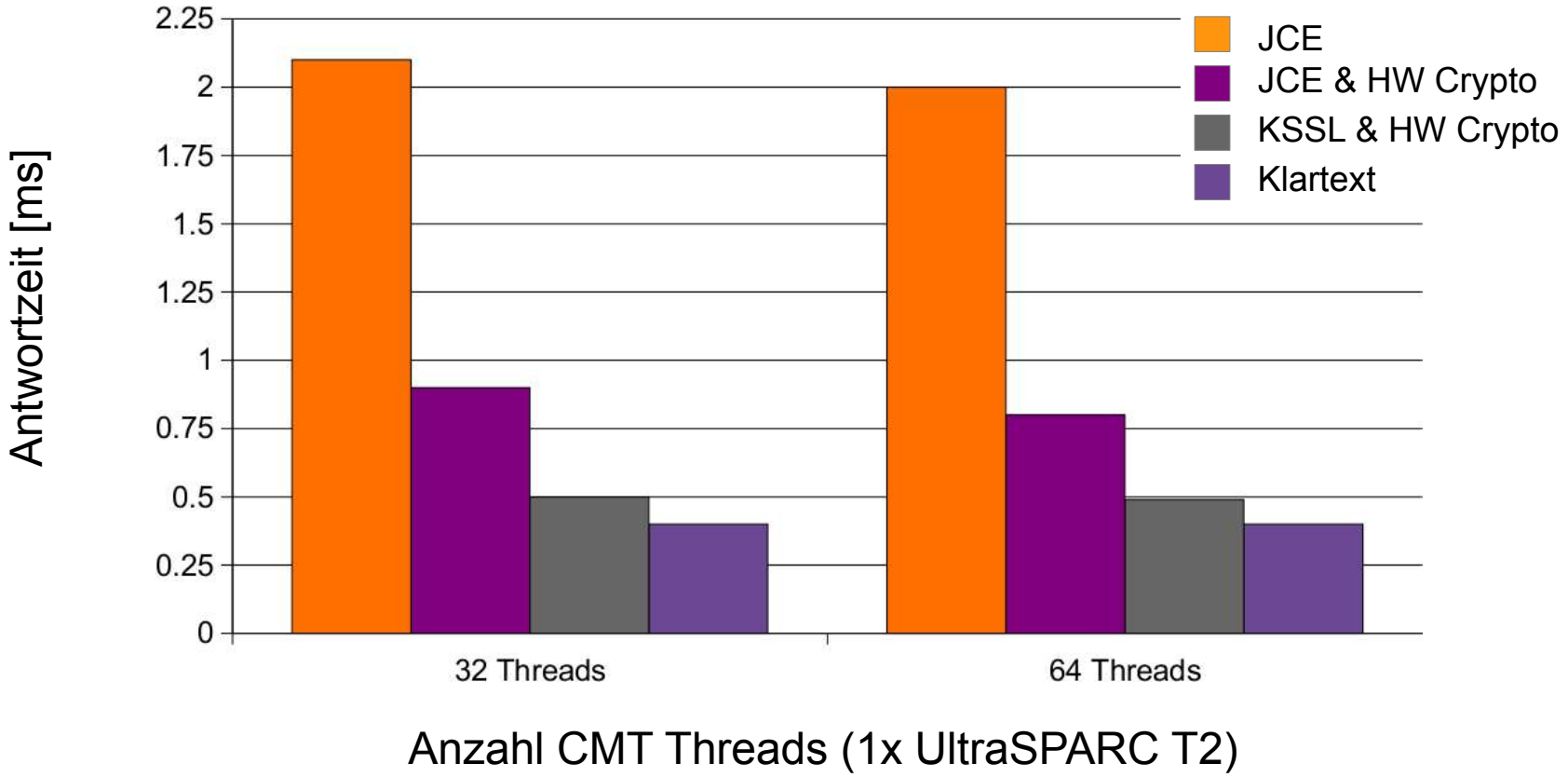
KSSL – Durchsatz

Aus einer Studie mit Weblogic



KSSL – Antwortzeit

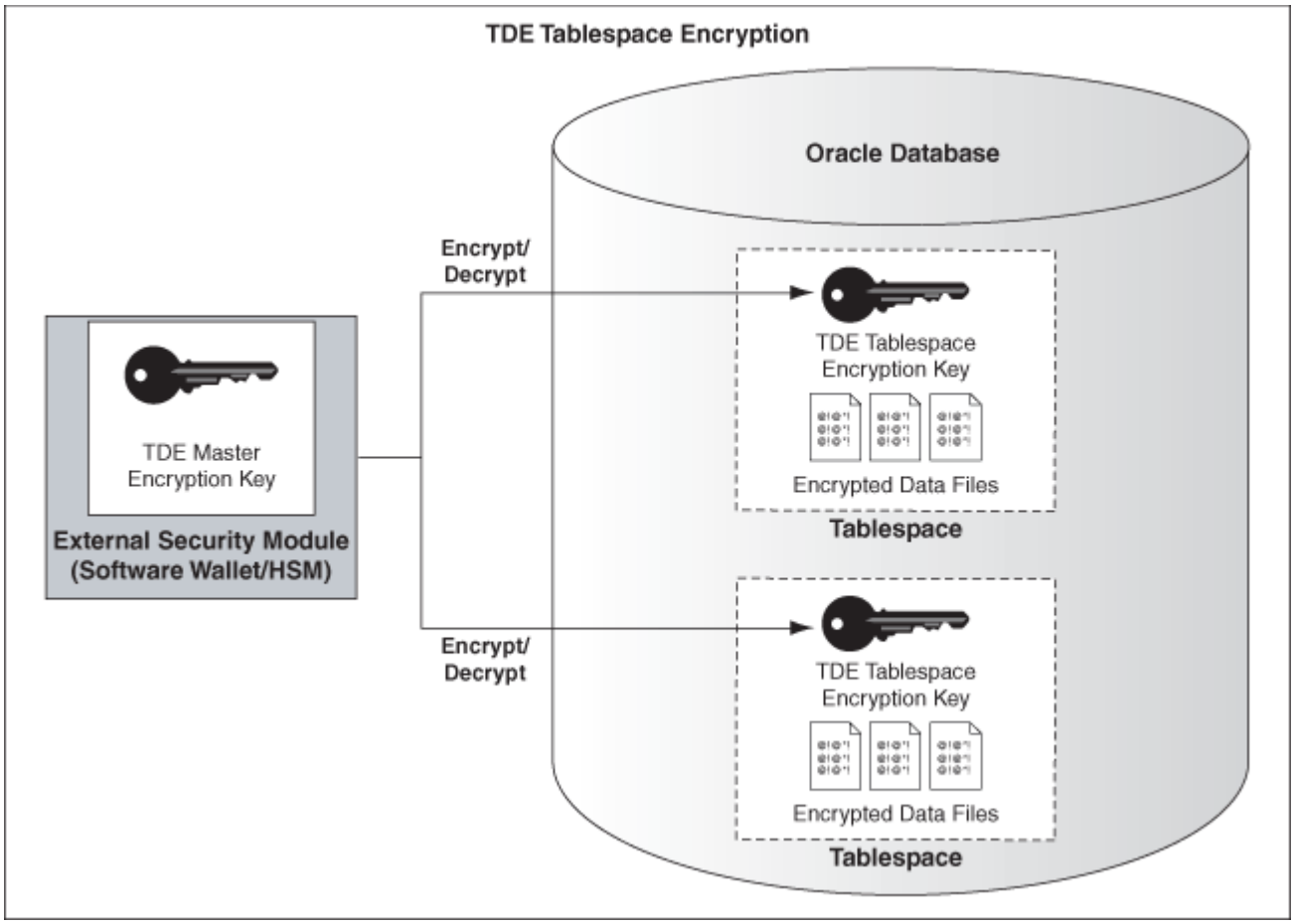
Aus einer Studie mit Weblogic



Beispiele – Oracle Transparent Data Encryption

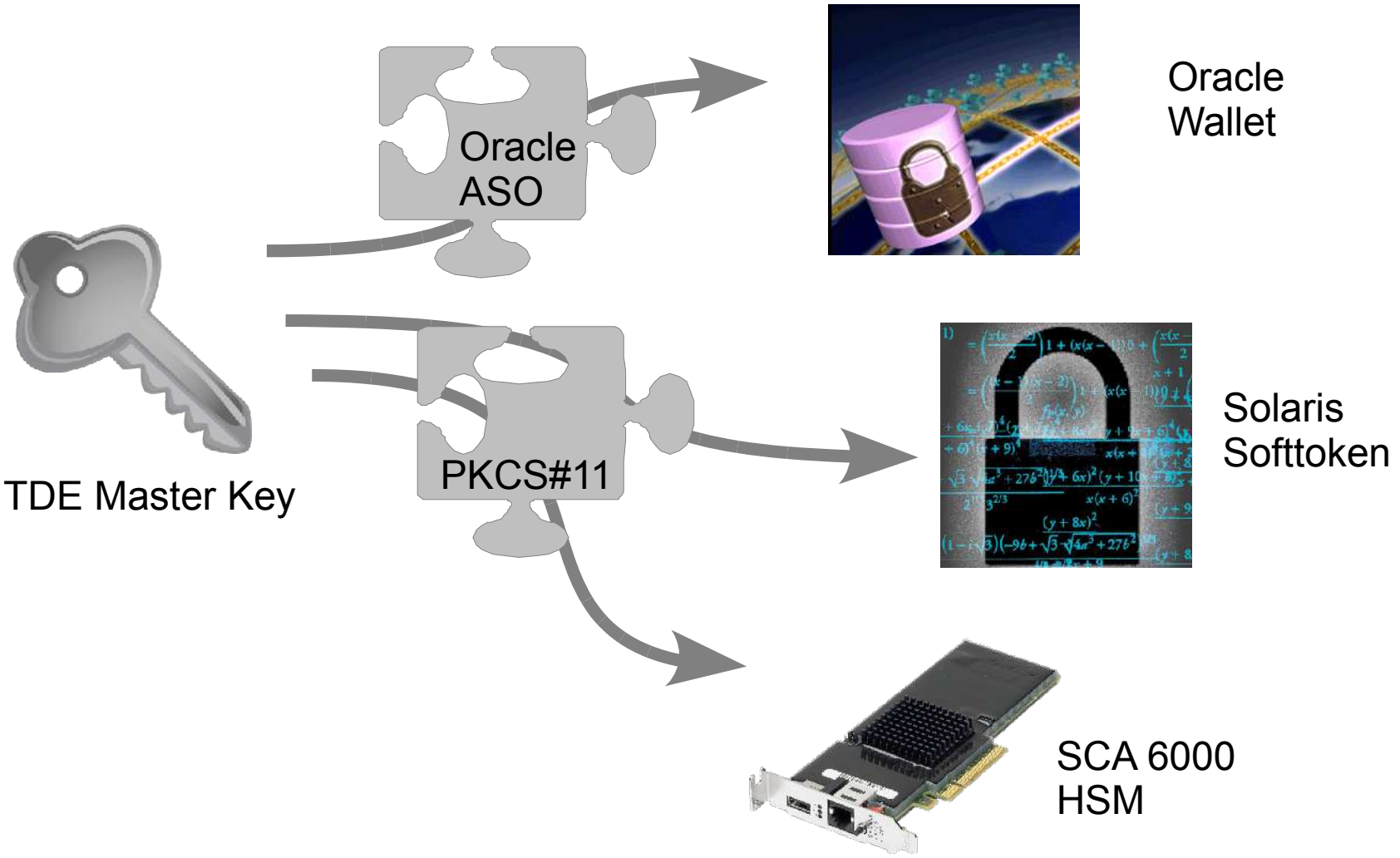
- TDE nutzt das Solaris Cryptographic Framework
  - als alternatives Wallet via PKCS#11
    - Solaris Softtoken
    - SCA 6000 HSM
  - Zur Beschleunigung der Verschlüsselung mit
    - SPARC T3
    - Intel Xeon 5600

Schlüssel bei Oracle TDE



Source: http://download.oracle.com/docs/cd/E11882_01/network.112/e10746/img/transdata_1.gif

Oracle TDE – Solaris Crypto Framework als Wallet



Solaris Crypto Framework als Wallet: So geht's

Oracle vorbereiten

- libpkcs11.so bekannt machen

```
mkdir -p /opt/oracle/extapi/32/hsm/sun/1.0.0
mkdir -p /opt/oracle/extapi/64/hsm/sun/1.0.0
cp /usr/lib/libpkcs11.so  \
    /opt/oracle/extapi/32/hsm/sun/1.0.0
cp /usr/lib/sparcv9/libpkcs11.so \
    /opt/oracle/extapi/64/hsm/sun/1.0.0
```

- ENCRYPTION_WALLET_LOCATION in sqlnet.ora

```
ENCRYPTION_WALLET_LOCATION=
  (SOURCE=(METHOD=HSM)(METHOD_DATA=
    (DIRECTORY=/some/place/for/my/wallet)))
```

Solaris Crypto Framework als Wallet: So geht's

Masterkey im Softtoken

- Softtoken initialisieren
  - pktool setpin (Als User “oracle”)
- Kein PKCS#11 Username
- Passwort für Oracle ist die “pin” von oben
- Optional:
  - “Token”-Dateien in ~/.sunw/pkcs11_softtoken
  - Erkundung des Softtoken mit “pktool”

Solaris Crypto Framework als Wallet: So geht's

Masterkey in SCA6000

- Karte gemäß Admin Guide installieren
- Karte initialisieren
  - scamgr -D
- Keystore anlegen
  - scamgr – Siehe Admin Guide
- PKCS#11 Username anlegen
  - scamgr – Siehe Admin Guide
- Passwort für Oracle ist “username:password”
- SCF konfigurieren

```
cryptoadm enable metaslot token=DOAG2010
cryptoadm disable metaslot auto-key-migrate
```

Solaris Crypto Framework als Wallet: So geht's

Masterkey Erzeugen

- Softtoken

```
sqlplus system/oracle
alter system set encryption key
   identified by "secret"
   migrate using “walletpwd” ;
```

- SCA 6000

```
sqlplus system/oracle
alter system set encryption key
   identified by "oracle:secret"
   migrate using “walletpwd” ;
```

Solaris Crypto Framework als Wallet: So geht's

Daten verschlüsseln

- Wallet öffnen und schließen

```
alter system set encryption
wallet open identified by “oracle:secret”;
```

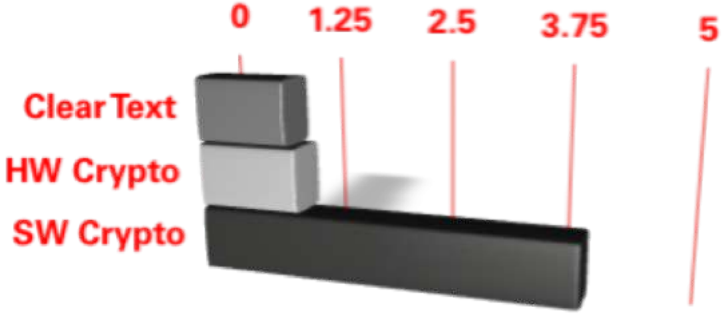
- Verschlüsseltes Tablespace anlegen

```
SQL> CREATE TABLESPACE securespace
  2  DATAFILE '+DATA/testdb/secure01.dbf'
  3  SIZE 150M
  4  ENCRYPTION
  5  DEFAULT STORAGE(ENCRYPT);
```

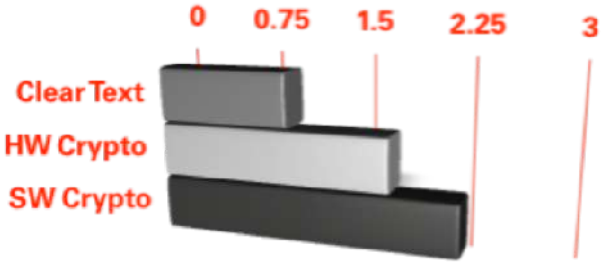
TDE Performance mit SPARC T3

Weniger als 10% Mehraufwand

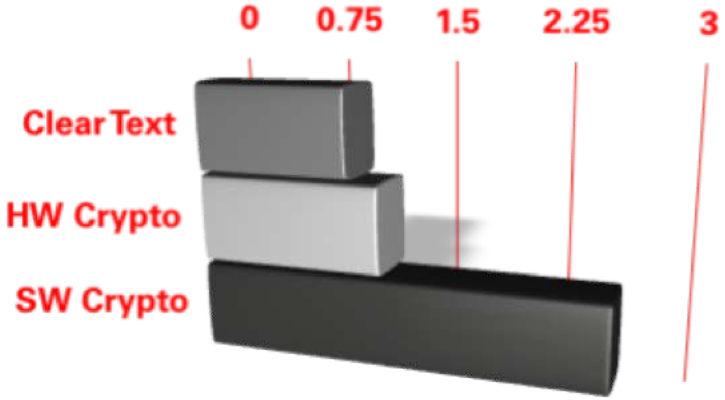
Table Load



Create Table as Select



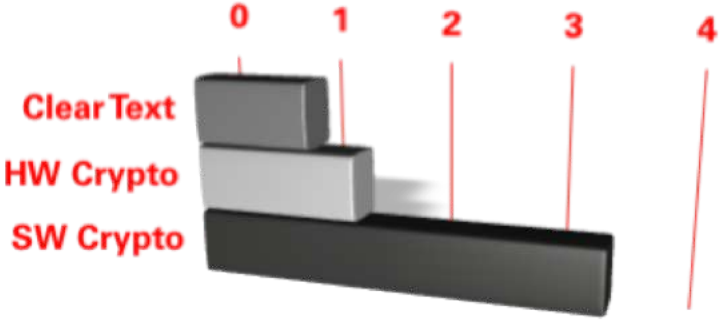
Index Creation



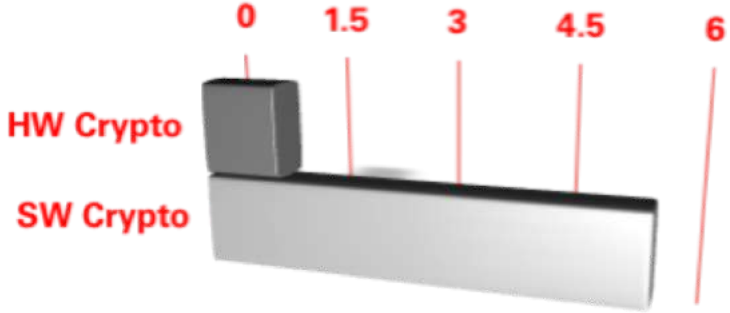
TDE Performance mit SPARC T3

T3 HW Crypto 3 bis 5 mal schneller als Software

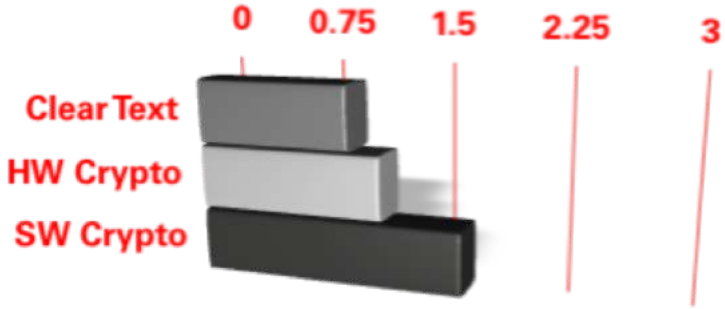
Join Table



Full Table Scan



Multi Table Hash Join



Solaris Cryptographic Framework

No Excuse for No Security

- Standardisierte Schnittstellen für
  - Anwendungs-Software
  - Software-Provider
  - Hardware-Provider
    - SCA 6000
    - T3 Crypto
    - 3rd Party wie bspw. nCipher oder Thales
- Breite Software-Unterstützung
  - KSSL, SSH, PKCS#11, OpenSSL, JCE
- Einfache Anwendung
  - cryptoadm, pktool, ksslcfg, openssl etc.

Hardware and Software

ORACLE

Engineered to Work Together

Appendix

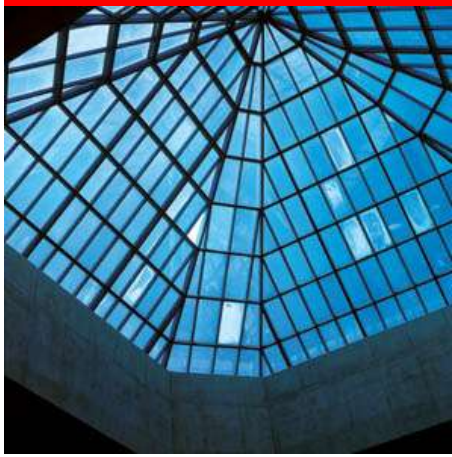

SPARC T3
ORACLE
©2010, Oracle®
SME 1912A LGA
07ALE3C701109
PG2.0.0
280 USA
2000-16
527-0000-01
1034

Referenzen

- Apache
  - http://www.sun.com/blueprints/0306/819-5782.pdf
- SSH
  - manpage zu sshd_config (4)
- Java
  - http://download.oracle.com/javase/6/docs/technotes/guides/security/index.html
- KSSL (am Beispiel von Weblogic)
  - http://www.oracle.com/technetwork/articles/systems-hardware-architecture/security-weblogic-t-series-168447.pdf

Substantiations

- SPARC Crypto Performance:
  - T2: http://wikis.sun.com/display/CryptoPerf/Competitive+performance
  - T3: http://blogs.sun.com/BestPerf/entry/20100920_sparc_t3_pk11rsaperf
- Intel Xeon 5600 AES Performance:
  - http://www.tomshardware.com/reviews/clarkdale-aes-ni-encryption,2538.html
- KSSL Performance:
  - http://www.oracle.com/technetwork/articles/systems-hardware-architecture/security-weblogic-t-series-168447.pdf
- T3 Crypto mit TDE
  - General Session mit John Fowler auf der OOW 2010



Appendix

- Encryption Legislation
- etc.

Examples of WW Government Mandates Requiring Encryption

- CA 1798 (formerly SB-1386) – California state regulation requiring public disclosure when unencrypted personal information is compromised
  - Safe Harbor: no need to notify customers if data was lost per state breach notification laws if in compliance with security encryption requirements
- HIPAA – U.S. health care regulation that has mandated the privacy of patients and the security of medical records, also known as protected health information (PHI).
- Personal Information Protection Act – Japanese regulation on information privacy
- Gramm-Leach-Bliley Act – U.S. finance industry regulation requiring public disclosure of personal data breaches
- EU Data Protection Directive – European Union directive on privacy and electronic communications
- National Data Privacy laws – Becoming pervasive in many nations, including Spain, Switzerland, Australia, Canada and Italy
- PCI – Payment Card Industry Data Security Standard – Globally governs all merchants and organizations that store, process or transmit this data
- The European Council and European Parliament appear to be moving towards legislation that would require all 27 EU Member States to introduce breach notice rules in accordance with the EU-level provisions (04/09) http://www.privacylaws.com/Documents/PL&B_INT_SPL/intnews98.pdf

Security Breach Costs Example

- TJMaxx
  - 45.7 Million customer records compromised starting in July 2005
  - Not discovered until Dec. 18, 2006
  - Hired outside investigators
  - Issued press release on Jan.17, 2007
  - Notified Securities and Exchange Commission in 2007 10K Annual Report
    - (http://www.sec.gov/Archives/edgar/data/109198/000095013507001906/b64407tje10vk.htm)
  - 17 pages in 10K Report devoted to breach extent, cost and litigation listings
  - T.J.Maxx had to absorb a charge of $135M related to the theft in first two quarters after discovery
- Card Systems
  - Potentially 40 Million records compromised in June, 2005
  - VISA USA has stopped allowing company to process card transactions
  - Company settled FTC charges by agreeing to security audits for the next 20 years

EU Data Protection Directive 95/46/EC

- Establishes set of requirements for processing personal data
- Requires each member state to transpose requirements into internal laws
  - As of July 13, 2007, all EU members have adopted individual laws
- Each EU member state has to setup supervisory authority to:
  - monitor data protection levels
  - advise government on regulations
  - start legal proceedings in case of violation
- Any entity processing data (“controller”) has to register with authority, and supply information about various aspect of processing, including security steps taken to protect data.
- Requires that third countries outside EU have adequate protection for any data being send to them.

EU Data Protection Directive 95/46/EC

EU Data Protection Directive Web Site

http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm

Member states laws & implementation status

http://ec.europa.eu/justice_home/fsj/privacy/law/implementation_e

APAC – Hong Kong Regulations

- Hong Kong Personal Data (Privacy) Ordinance
  - Went into force Dec. 20, 1996
  - Established Office of Privacy Commissioner for Personal Data
  - Governs the use of any data applying directly or indirectly to a living individual
  - Applies to any person that controls the collection, holding, processing or use of personal data
  - Principle 4 requires appropriate security measures to be applied to personal data
  - Visit Info Centre for sample of actions taken by PCPD to enforce this regulation
    - http://www.pcpd.org.hk/english/infocentre/press.html
  - PCPD Home Page
    - http://www.pcpd.org.hk/english/ordinance/ordglance.html

APAC - Japan Regulations

Japan Personal Information Protection Act (JPIPA)

- Enacted in 2003, in force since April 1, 2005
- Applies to any organization using database of 5000 or more individuals
- Regulates acquisition, handling and usage of personal information
- Business regulated by Financial Services Agency have to publicize any data leaks

US Federal Data Security Laws

- Gramm-Leach-Bliley Act (GLBA)
  - Applies to all financial institutions – private and public
  - Safeguards Rule requires companies to specify how they protect non-public information, and how they will continue to do so in the future
- Health Insurance Portability and Accountability Act (HIPAA)
  - Applies to any health care plans and providers processing health care data in electronic form
  - Requires protection of medical information privacy
  - http://www.hhs.gov/ocr/hipaa/

US State/Other Regulations

State Laws

- California SB1386
  - Requires notification to any customer whose unencrypted data has been acquired to unauthorized person.
- Number of other state bills modeled after California SB1386
  - Massachusetts Data Security Regulations
  - Minnesota Statue 365E.64
  - Texas HB3222
  - Illinois SB 1675
  - Nevada NRS 597.970

PCI DSS – Payment Card Industry Data Security Standard

- Any company transmitting, processing or storing payment card data must be PCI DSS compliant
- Requirement 3 specifies all details for stored data protection

Canada Security Law (PIPEDA)

Personal Information Protection and Electronics Documents Act (PIPEDA)

Established office of Privacy Commissioner

Governs how organizations collect, use and disclose personal data

Dictates that data be protected by security safeguards based on the sensitivity of the information

Complaints result in investigation, followed by non-binding report.

Commision has ability to make any information related to investigation public

http://www.ic.gc.ca/epic/site/ecic-ceac.nsf/en/h_gv00464e.html

Enterprise Security Survey

73% of people surveyed in enterprise market have interest in encrypting disk/tape - #3 after network access control and content filtering

Top three IT security evaluation factors are*:

- Security of product – 84%
- Scalability/performance - 79%
- Best price/performance - 78%

Top three priorities*:

- Protect customer data - 82%
- Business continuity - 76%
- Protection of corporate intellectual property - 75%

* “The State of Enterprise IT Security Adoption:2007” - Jonathan Penn, Forrester Research Inc.

SMB Security Survey

60% of people surveyed in SMB market have interest in encrypting disk/tape - higher than any technology other than content filtering

Top three IT security evaluation factors are*:

- Security of product – 84%
- Simplest manageability – 77%
- Best price/performance

Top three concerns:

- Loss of customer data
- Financial fraud
- Theft of intellectual property

* “The State of SMB IT Security Adoption:2007” - Jonathan Penn, Forrester Research Inc.