Applying Oracle Technologies in PCI DSS certification process

Ilonka Duka, dipl. ing.ele.
IT Infrastruktura
Splitska Banka Societe Générale d.d.
ilonka.duka@splitskabanka.hr

SPLITSKA BANKA
SOCIETE GENERALE GROUP

Agenda

- Introduction: SGSB, PCI DSS standard and Oracle
- Transparent Data Encryption Performance Testing:

  project goals, business activity simulation and test cases,

  testing platform architecture, performance indicators
- TDE Performance Testing: Test results

Societe Générale Splitska Banka

- Member of Societe Générale Group, strong financial institution operating as a universal bank on Croatian banking market, holding a 8.5% market share and having 1550 employees.
- 121 branches, 500,000 individual clients and 25,000 corporate clients
- Vision: to be one of the leading Croatian banks with the support of a major European banking group, with customer-oriented staff and unique and efficient processes and technologies.

SPLITSKA BANKA
SOCIETE GENERALE GROUP

Societe Générale Splitska Banka

- In process of migrating to the new core banking system, using Oracle database software (10gR2 on AIX)

- In process of acquiring PCI DSS certificate (VISA)

SPLITSKA BANKA
SOCIETE GENERALE GROUP

PCI DSS – Payment Card Industry Data Security Standard

- Set of comprehensive requirements for enhancing payment account data security
- Developed and maintained by the founding payment brands of PCI Security Standards Council
- To facilitate consistent data security measures and prevent credit card fraud through increased data and procedures controls

PCI DSS Requirements

Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data
	2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data
	4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software on all systems commonly affected by malware
	6. Develop and maintain secure systems and applications

PCI DSS Requirements

Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need-to-know
	8. Assign a unique ID to each person with computer access
	9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data
	11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security

PCI DSS and Oracle

- Oracle Database implementation that stores, processes,

  or transmits cardholder data - in the scope of PCI DSS compliance

- Requirement 3: protect stored cardholder data

  (Oracle Advanced Security Transparent Data Encryption - TDE)

PCI DSS and Oracle

- Payment Card Industry, PCI DSS Requirement 3.4
  Requirement 3: Protect stored cardholder data

3.4	Render PAN, at minimum, unreadable anywhere it is stored (including data on portable digital media, in logs, and data received from or stored by wireless networks)
3.4.1	If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed independently of native operating system access control mechanisms (for example, by not using local system or Active Directory accounts). Decryption keys must not be tied to user accounts.
3.5	Protect encryption keys used for encryption of cardholder data against both disclosure and misuse
3.5.1	Restrict access to keys to the fewest number of custodians necessary
3.5.2	Store keys securely in the fewest possible locations and forms.

PCI DSS and Oracle

- 3.6 Fully document and implement all key management processes and procedures for keys used for encryption of cardholder data, including generation of strong keys, secure key distribution, secure key storage, periodic changing of keys
  - 3.6.5 Destruction of old keys
  - 3.6.6 Split knowledge and establishment of dual control of keys (so that it requires two or three people, each knowing only their part of the key to reconstruct the whole key)
  - 3.6.7 Prevention of unauthorized substitution of keys
  - 3.6.8 Replacement of known or suspected compromised keys
  - 3.6.9 Revocation of old or invalid keys
  - 3.6.10 Requirement for key custodians to sign a form stating that they understand and accept their key-custodian responsibilities.

PCI DSS and Oracle

- Oracle DBMS Obfuscation Toolkit (DOTK) (Oracle 8g & 9g)

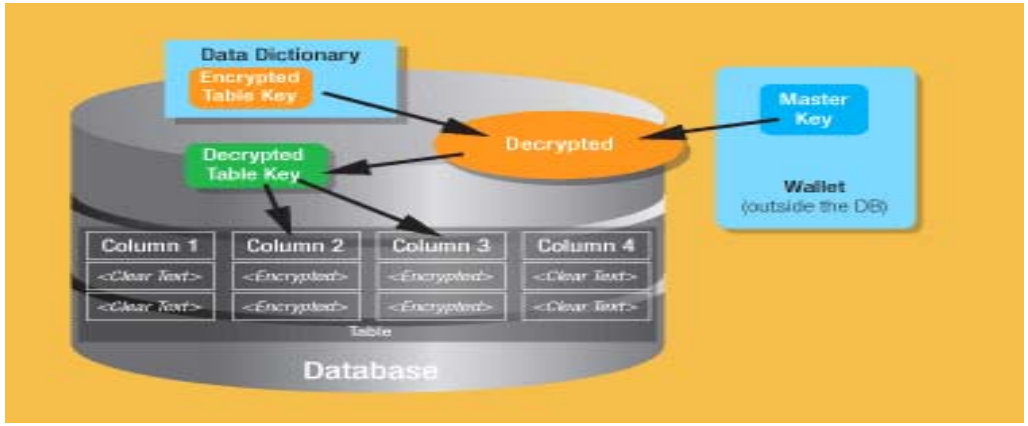
  Oracle DBMS_CRYPTO package

  Oracle Advanced Security Option:

  Oracle Transparent Data Encryption (TDE)

  Oracle Database Vault

Oracle TDE



- Native database solution completely transparent to existing applications (no triggers, views, or other application changes required)

  Data is transparently encrypted when written to disk and transparently decrypted after an application user has successfully authenticated and passed all authorization checks.

  10g – Column Level Encryption vs. 11g – Tablespace Level Encryption

TDE setup

- TDE – Oracle 10g EE Advanced Security option

  Specify wallet location, open the wallet

  Copy table mocarte_nocrypt to mocart_crypt (AES128) and mocarte_crypt2 (AES256) and encrypt columns (one column per table), no salt option

  Initial “feel” testing: copy tables, data pump export

Data Encription Performance Testing

- Client and End user of Card System
- Societe Générale BHFM/DSI/ATR – Project Coordination
- External Benchmark Expert

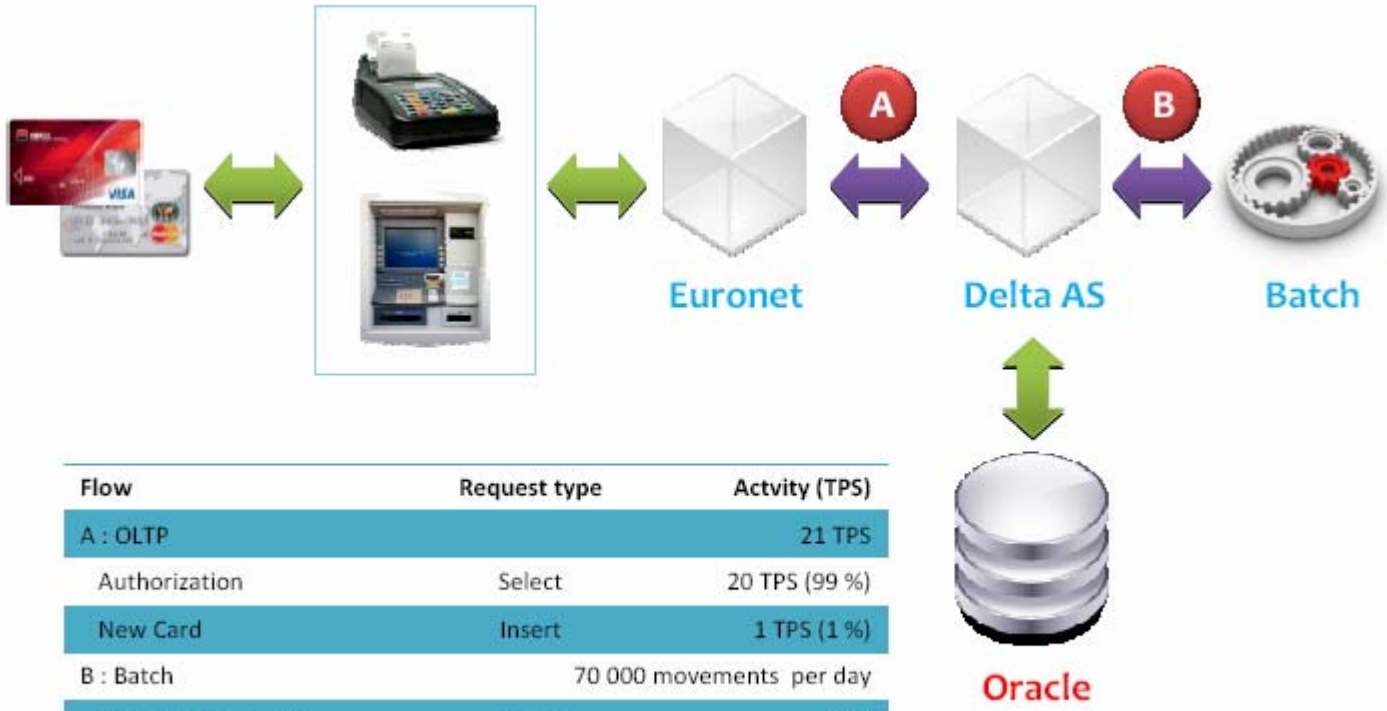
Project Goal

- Analysis the performance impact of TDE (Oracle Data Encryption) on the DeltaBank Card Management system
  - Impact on OLTP activities
  - Impact on Batch activities
  - Oracle Auditing performance impact
  - Oracle infrastructure overhead
- Scalability and limit testing
  - DeltaBank Card Management system future performance with Data Encryption
- Recommendations
  - Oracle & DeltaBank Application parameter tuning

Test cases

- I: Performance Baseline without Oracle Data Encryption (2009 vol.)
  - T1 : SELECT (20 to 1000 TPS, 1 to 8 Oracle Connections)
  - T2 : UPDATE (20 to 100 TPS, 1 to 8 Oracle Connections)
  - T3 : INSERT (20 to 100 TPS, 1 to 8 Oracle Connections)
  - T4 : SELECT + UPDATE + INSERT (20 to 1200 TPS, 1 to 8 Oracle Connections)
- II: Performance Baseline with Oracle Data Encryption
  - T5 : SELECT (20 to 1000 TPS, 1 to 8 Oracle Connections)
  - T6 : UPDATE (20 to 100 TPS, 1 to 8 Oracle Connections)
  - T7 : INSERT (20 to 100 TPS, 1 to 8 Oracle Connections)
  - T8 : SELECT + UPDATE + INSERT (20 to 1200 TPS, 1 to 8 Oracle Connections)
- III: Capacity planning with Oracle Data Encryption (2011 volume)
  - T10 : SELECT (20 to 1000 TPS, 1 to 8 Oracle Connections)
  - T11 : UPDATE (20 to 100 TPS, 1 to 8 Oracle Connections)
  - T12 : INSERT (20 to 100 TPS, 1 to 8 Oracle Connections)
  - T14 : SELECT + UPDATE + INSERT (20 to 1200 TPS, 1 to 8 Oracle Connections)

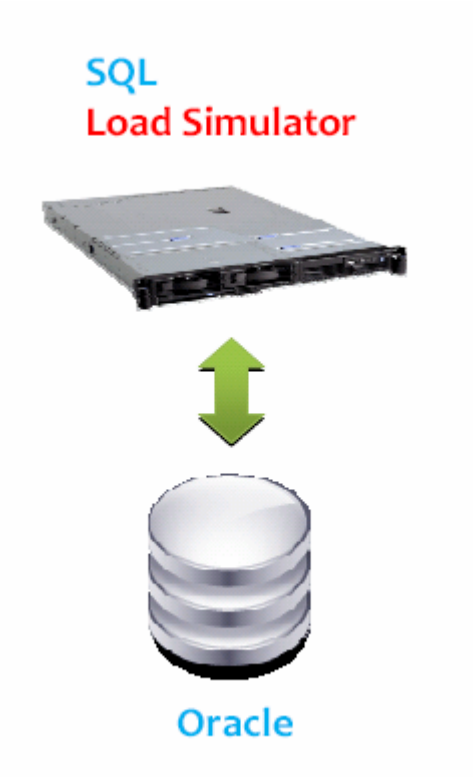
Business transaction activity & Flow



Flow	Request type	Actvity (TPS)
A : OLTP		21 TPS
Authorization	Select	20 TPS (99 %)
New Card	Insert	1 TPS (1 %)
B : Batch		70 000 movements per day
Booking Transaction	Select	99%
New card confirmation	Update	1 %
A + B (in peak)	Select + Update + Insert	270 TPS

SPLITSKA BANKA
SOCIETE GENERALE GROUP

Testing platform architecture



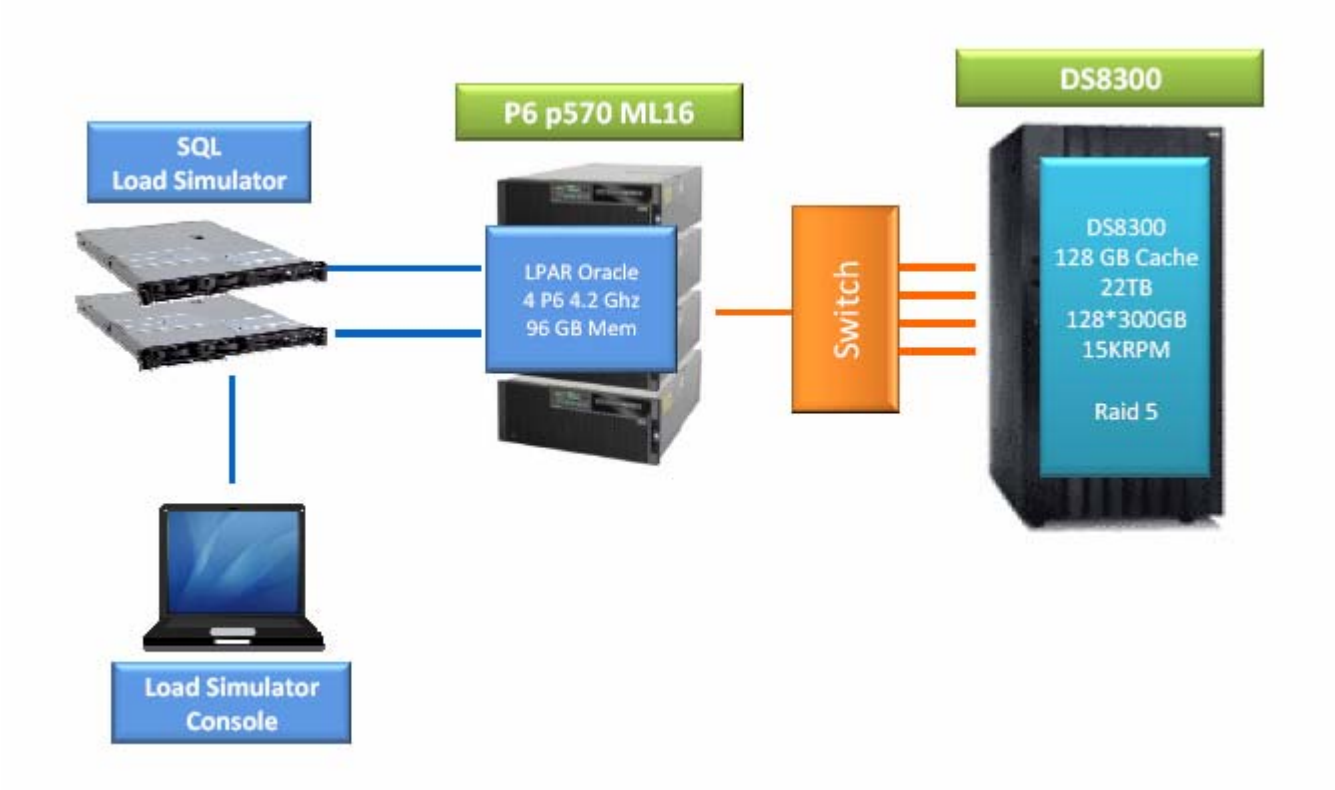
Borland SilkPerformer - software-application performance, load, and stress testing.

Customized load tests

SilkPerformer's reporting tools

(Silk Performance Explorer)

Testing platform technical infrastructure



Performance indicators

- Response Time
  - SELECT
  - UPDATE
  - INSERT

- Oracle Server Resource Utilization
  - CPU
  - Memory

Defining customized load tests

File Edit Record Script Project Run Results Tools View Settings Window Help

Outline Project | Model Script | Try Script | Customize Test | Find Baseline | Confirm Baseline | Adjust Workload | Run Test | Explore Results | Reuse Project

Project

- Project 'SGSB'
  - Profiles
  - Scripts (6)
    - BATCH2.bdf (C:\Program Files\Borland\SilkPerformer 2009\Working\Proje
    - BATCH3_SELECT.bdf (C:\Program Files\Borland\SilkPerformer 2009\Work
    - BATCH3_UPDATE.bdf (C:\Program Files\Borland\SilkPerformer 2009\Wor
    - BATCH4.bdf (C:\Program Files\Borland\SilkPerformer 2009\Working\Proje
    - NEW_CARD.bdf (C:\Program Files\Borland\SilkPerformer 2009\Working\P
    - TDE_SGSB.bdf (C:\Program Files\Borland\SilkPerformer 2009\Working\Pro
  - Include Files (5)
    - db.bdh (c:\program files\borland\silkperformer 2009\working\include\)
    - kernel.bdh (c:\program files\borland\silkperformer 2009\working\include\)
    - measurebounds.bdh (c:\program files\borland\silkperformer 2009\workin
    - ora.bdh (c:\program files\borland\silkperformer 2009\working\include\)
    - ora8.bdh (c:\program files\borland\silkperformer 2009\working\include\)
  - Data Files (4)
    - B3_CRYPT.csv (C:\Program Files\Borland\SilkPerformer 2009\Working\Da
    - B3_NOCRYPT.csv (C:\Program Files\Borland\SilkPerformer 2009\Working
    - BKCLI.CSV (C:\Program Files\Borland\SilkPerformer 2009\Working\Data\)
    - cli.csv (C:\Program Files\Borland\SilkPerformer 2009\Working\Data\)
  - Agents
  - Workloads (8)
    - **BATCH2**
    - BATCH3 SELECT CRYPT
    - BATCH3 SELECT NOC
    - BATCH3 UPDATE CRYPT
    - BATCH3 UPDATE NOC
    - BATCH4_SELECT_C
    - New Card
    - Workload1

Project | Results | Active Script

BATCH2.bdf

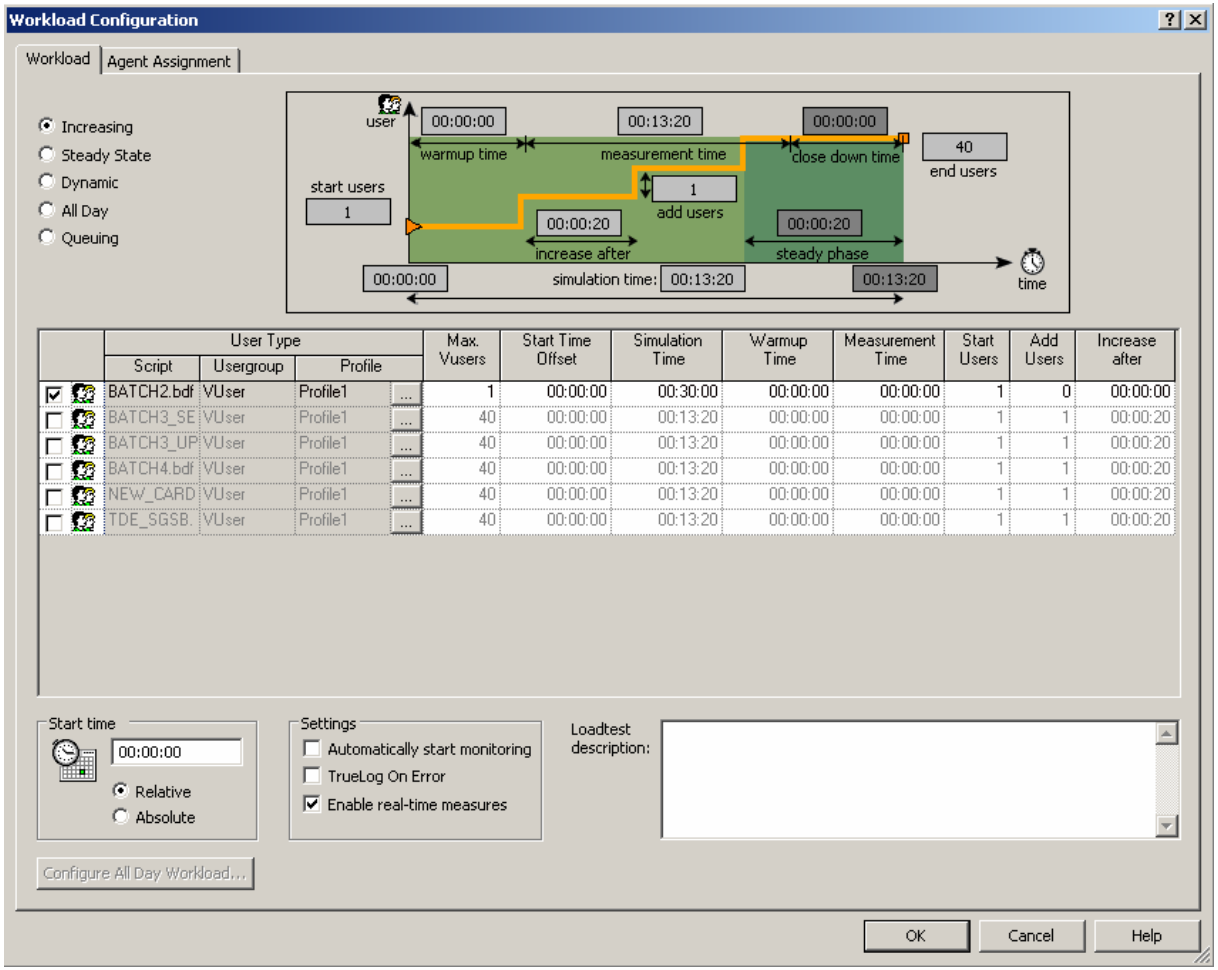
```
//-----------------------------------------------------------------------
// Recorded 14/09/2009 by SilkPerformer Recorder v7.9.0.3643
//-----------------------------------------------------------------------
// Rule set "ASP.NET ViewState"
//   * Rule "Parse and Replace __VIEWSTATE"
//   * Rule "Parse and Replace __EVENTVALIDATION"
//-----------------------------------------------------------------------
@codepage(1250)

benchmark SilkPerformerRecorder

use "Kernel.bdh"
use "Ora8.bdh"

const
    CONNECTSTR     :="pcidss/pcidss@DLTSGSB";

dclparam
    strCLI       : string;
    strAGE       : string;
    strDEV       : string;
    strNCP       : string;
    strNCART     : string;
    strREFCAR    : string;


dcluser
  user
    VUser
  transactions
    TInit            : begin;
    TMain            : 1;
    TShutdown        : end;

var

  hConnect           : number;
  fetched            : number;

  c1                 : cursor;

dclrand
```

Output

Compiler | Virtual User | Simulation Controller

SPLITSKA BANKA
SOCIETE GENERALE GROUP

Executing load tests



SPLITSKA BANKA
SOCIETE GENERALE GROUP

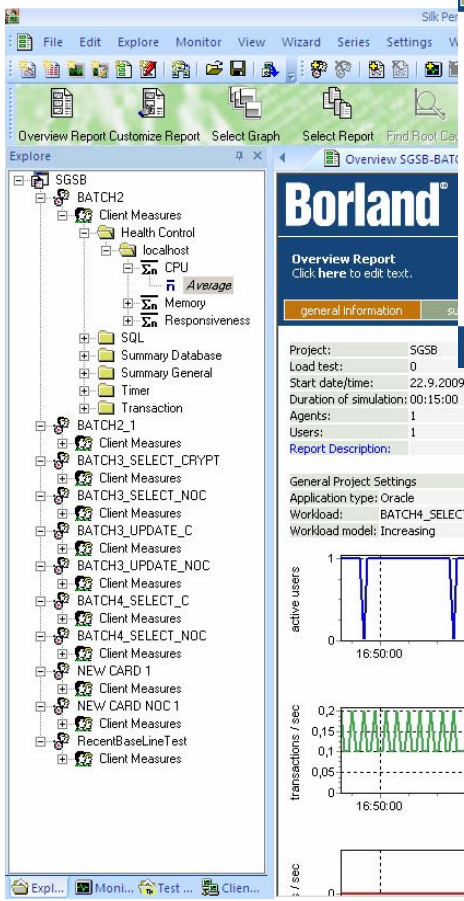
Results

Results forBATCH3_SELECT.bdf/¥User/Profile1_1 back to overview

summary tables | transactions | custom timers | database

The custom timer measurement group contains timers that are defined in the load-testing script. For each timer that is started with the MeasureStart function, a time measurement is displayed; the measurement name is taken from the first parameter that is passed to the MeasureStart function.

Name	Avg	Min	Max	Count	Measured	StdDev	Bound1	Bound2
#Overall Response Time#								
Response time[s]	5,802	5,767	5,837	2	2	0,035		
Check if card exists Crypt								
Response time[s]	5,837	5,837	5,837	1	1	0,000		
Checking if card exist NoCrypt								
Response time[s]	5,767	5,767	5,767	1	1	0,000		



Borland

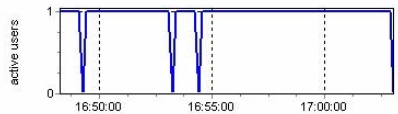
Overview Report
Click **here** to edit text.

general information

Results forBATCH3_SELECT.bdf/¥User/Profile1_1 back to overview

Project:	SGSB
Load test:	0
Start date/time:	22.9.2009 16:48:04
Duration of simulation:	00:15:00
Agents:	1
Users:	1
Report Description:	

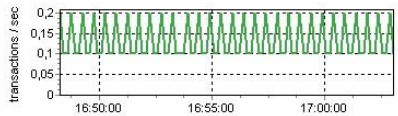
General Project Settings
Application type: Oracle
Workload: BATCH4_SELECT_C
Workload model: Increasing



Active Users

This chart shows the overall number of active virtual users. A virtual user is considered as active if the user has started and is currently in one of the following states: executing, wait DB, document downloading, and thinktime.
Click here to edit text.

number of concurrent users: 1



Transactions

The number of SilkPerformer transactions per second.
Click here to edit text.

number of transactions: 120
average number of transactions/sec: 0,13

Errors

This chart shows the number of API errors per second, including Internet, database, and middleware

SPLITSKA BANKA
SOCIETE GENERALE GROUP

Conclusions and recommendations

- Bulk operations (expdp, copy lines, sorting by encrypted column) – high response times increase

- Realistic batch processing (example loads) – no significant response time, performance or server stress difference

Questions?

SPLITSKA BANKA
SOCIETE GENERALE GROUP

Thank you for your attention

Ilonka Duka, dipl. ing.ele.
IT Infrastruktura
Splitska Banka Societe Générale d.d.
ilonka.duka@splitskabanka.hr

SPLITSKA BANKA
SOCIETE GENERALE GROUP