LSA & Safety - RBAC, MCS

V.Kain, S. Gysin, G. Kruk, M. Lamont, J. Netzel, A. Rey,
W. Sliwinski, M. Sobczak, J. Wenninger

- Roled Based Access Control (RBAC)
  - How to protect equipment properties from unauthorized access
- Management of Critical Settings (MCS)
  - How to protect settings from changes by unauthorized personnel

Contents

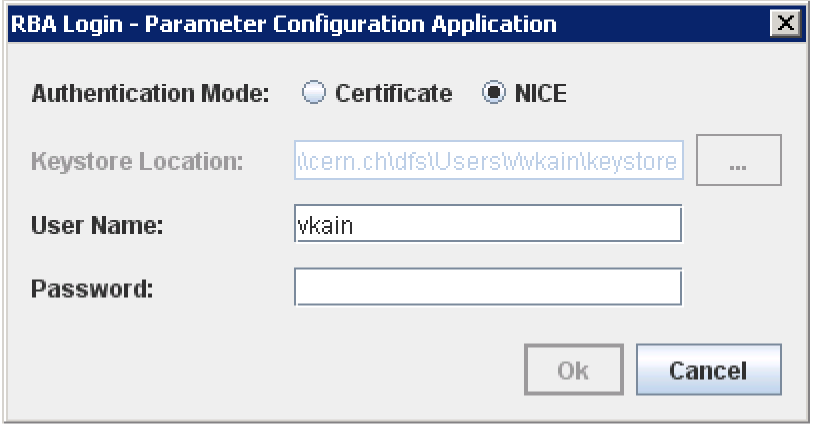
- Introduction of concepts – VK
- Integration of RBAC and MCS in the LHC control system – W. Sliwinski

Motivation – LSA Security (1)

- Operational errors can lead to magnet quenches → long recovery times → impact on machine performance

- Enormous energy stored in magnets and beams → uncontrolled release of this energy car ent → even longer down-times

- To cope with this



RBA Login - Parameter Configuration Application

Authentication Mode: ○ Certificate ● NICE

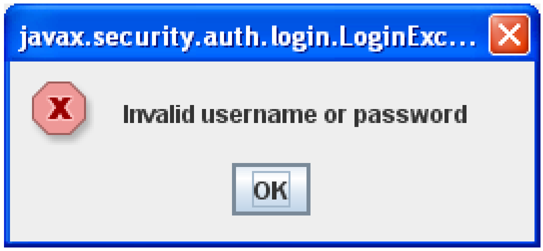
Keystore Location: \\cern.ch\dfs\Users\v\vkain\keystore

User Name: vkain

Password:

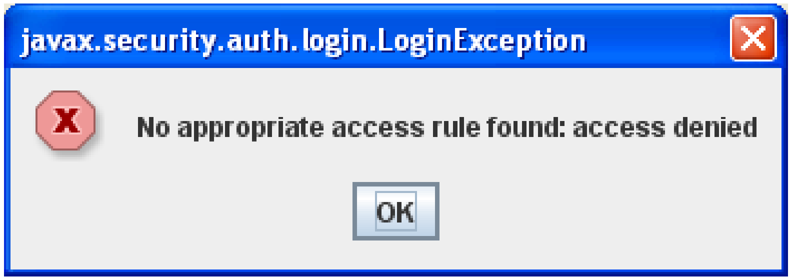
- Plus: the requirement for a **cultural change** during LHC operation

sed to **login**



javax.security.auth.login.LoginExc...

Invalid username or password



javax.security.auth.login.LoginException

No appropriate access rule found: access denied

Motivation – LSA Security (2)

- Need to prevent:
  - Well meaning person fr ng thing at the wrong moment
  - Ignorant per ything at any moment

Role Based Access

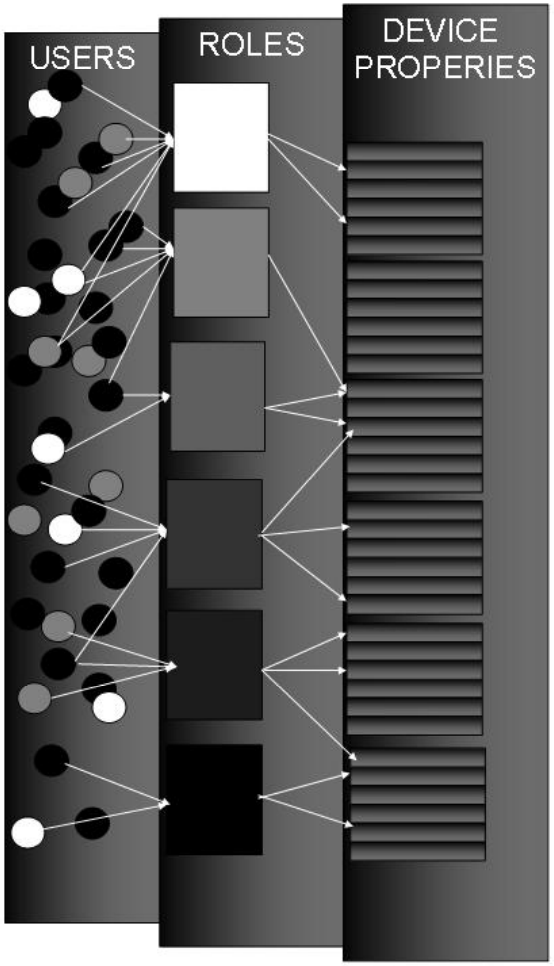
- Need to provide:
  - Critical parameters whic machine are what they are su d by an authorized person a

Management of Critical Settings

Role Based Access Control (RBAC)

- LAFS collaboration – S. Gysin

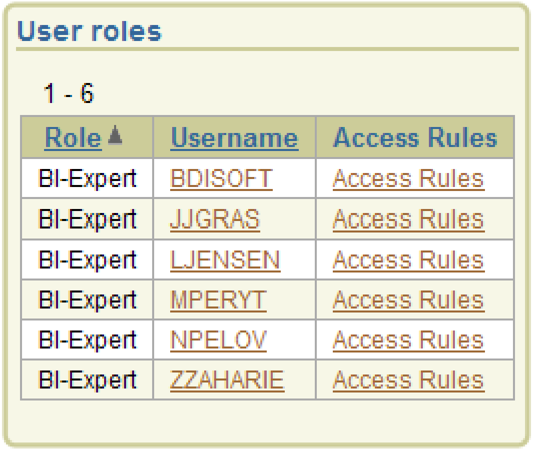
- RBAC works by giving people **ROLES** and assigning ROLES **PERMISSIONS** to access device properties



- So, it provides means for
  - AUTHENTICATION
    - Interfaces to NICE DB: login with nice ID and password
    - The Roles for that user name are allocated
    - An RBAC token is issued
  - AUTHORISATION
    - Access Maps are built by the equipment owners/responsible which are stored on the front-ends
    - Access maps contain the **Access Rules**
    - RBAC is part of CMW

Management of Roles and Rules

- Each role has an administrator
  - Administrator is responsible for keeping membership up-to-date

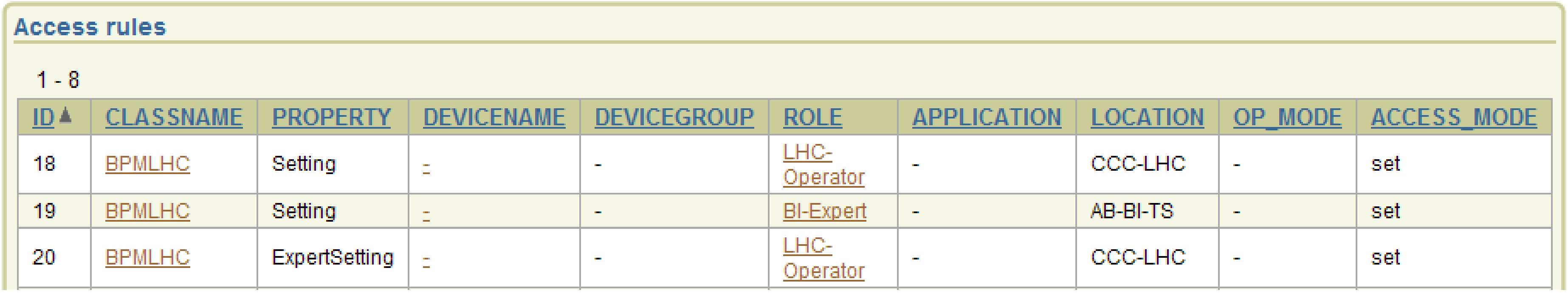


User roles

1 - 6

Role ▲	Username	Access Rules
BI-Expert	BDISOFT	Access Rules
BI-Expert	JJGRAS	Access Rules
BI-Expert	LJENSEN	Access Rules
BI-Expert	MPERYT	Access Rules
BI-Expert	NPELOV	Access Rules
BI-Expert	ZZAHARIE	Access Rules

- Each equipment class has an administrator – equipment owners
  - The administrator defines the rules for certain roles



Access rules

1 - 8

ID ▲	CLASSNAME	PROPERTY	DEVICENAME	DEVICEGROUP	ROLE	APPLICATION	LOCATION	OP_MODE	ACCESS_MODE
18	BPMLHC	Setting	-	-	LHC-Operator	-	CCC-LHC	-	set
19	BPMLHC	Setting	-	-	BI-Expert	-	AB-BI-TS	-	set
20	BPMLHC	ExpertSetting	-	-	LHC-Operator	-	CCC-LHC	-	set

Management of Critical Settings (MCS)

- Management of Critical Settings provides:
  - Critical parameters which can compromise the safety of the machine are what they are supposed be and can only be changed by an authorized person and nobody else
  - ➡ needs Authentication
  - ➡ needs Authorization

  } ➡ MCS uses RBAC

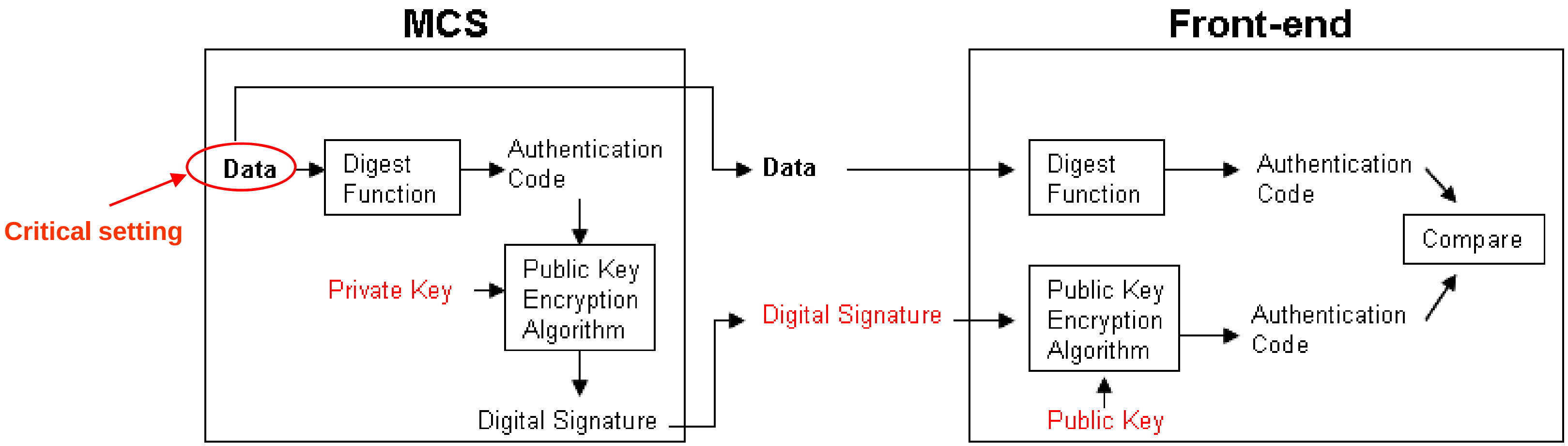
  - …and to be able to verify that value of the critical parameters has not changed since the authorized person has updated it
    - Through maliciousness – hacking
    - Through data corruption – radiation,…

  MCS **signs** the data with a unique signature

- MCS uses RBAC and public-private key digital signatures

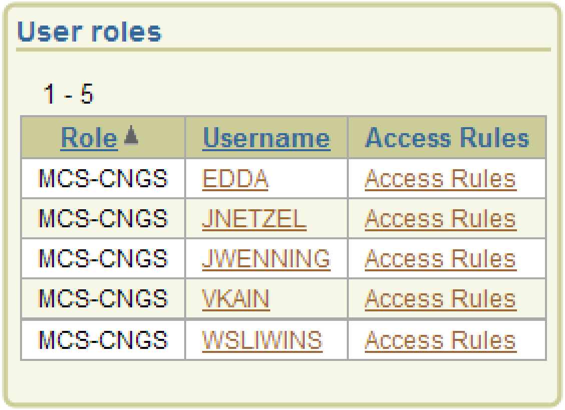
MCS – Digital Signatures

- Private key ….is secret. Only the authorized person can use it.
- Public key…everybody can have it. Stored on the front-end in a configuration file with the definition of the critical property.



- RBAC does the **key management for MCS:** **generation, storage, management**
  - Concept of **Critical Roles:** a role associated with a unique public-private key pair. Naming convention “MCS-xyz”
- RBAC extended its original scope to a large extend for MCS
  - **RBAC signs for MCS**

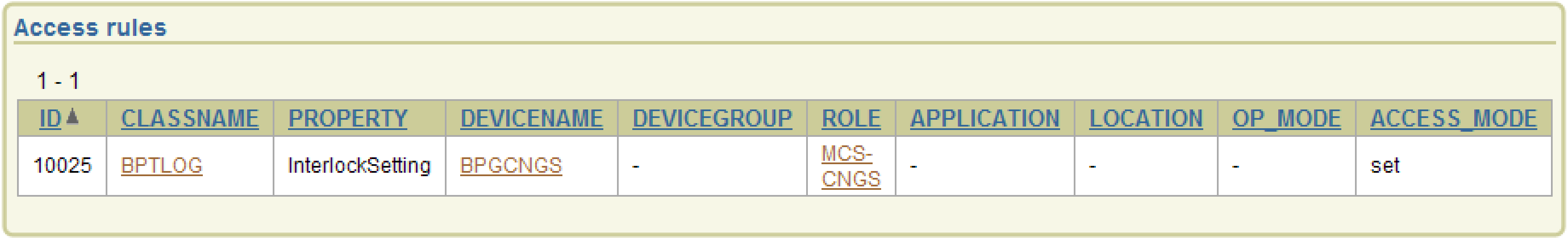
RBAC for MCS



User roles

1 - 5

Role ▲	Username	Access Rules
MCS-CNGS	EDDA	Access Rules
MCS-CNGS	JNETZEL	Access Rules
MCS-CNGS	JWENNING	Access Rules
MCS-CNGS	VKAIN	Access Rules
MCS-CNGS	WSLIWINS	Access Rules



Access rules

1 - 1

ID ▲	CLASSNAME	PROPERTY	DEVICENAME	DEVICEGROUP	ROLE	APPLICATION	LOCATION	OP_MODE	ACCESS_MODE
10025	BPTLOG	InterlockSetting	BPGCNGS	-	MCS-CNGS	-	-	-	set

Public key from RBAC for MCS-CNGS:

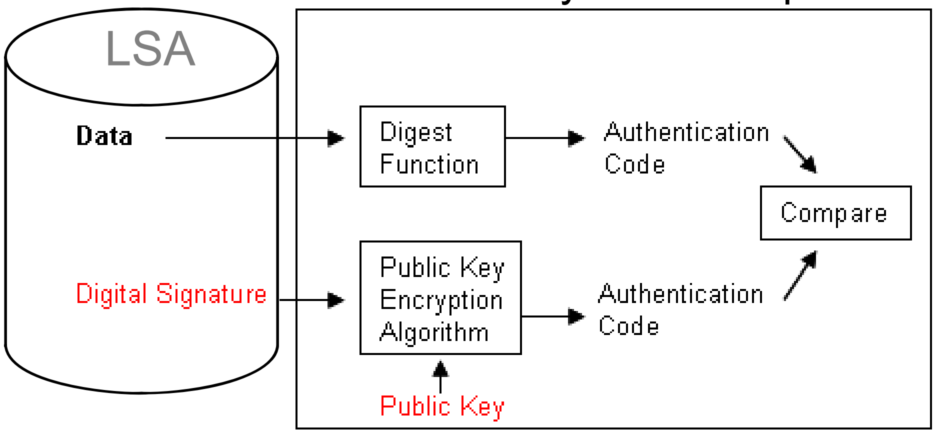
```
Sun RSA public key, 512 bits
  modulus:
822051788094408479372688686168452181258355438054036212654155680312497982110513545442424281504918237688
8878842206424573705934510869455619570409135604472299
  public exponent: 65537
```

What is a critical setting?

- A critical setting is an LSA setting stored in the LSA DB with the attribute “critical” and with a signature field
- **The integrity of a critical setting in the LSA DB can always be verified:**
  - ➡ LSA DB is the “TRUE” source for critical settings

Anybody can get the public key (SIS, sequencer). Private key only through the correct role.

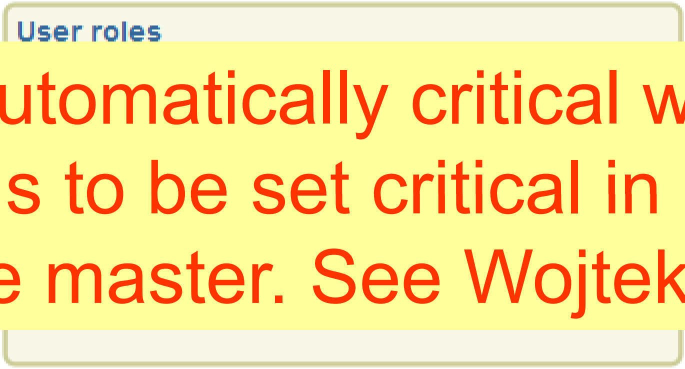
Check done by SIS or sequencer



- **Critical settings in the LSA DB are compared against critical settings in the hardware** → SIS, sequencer

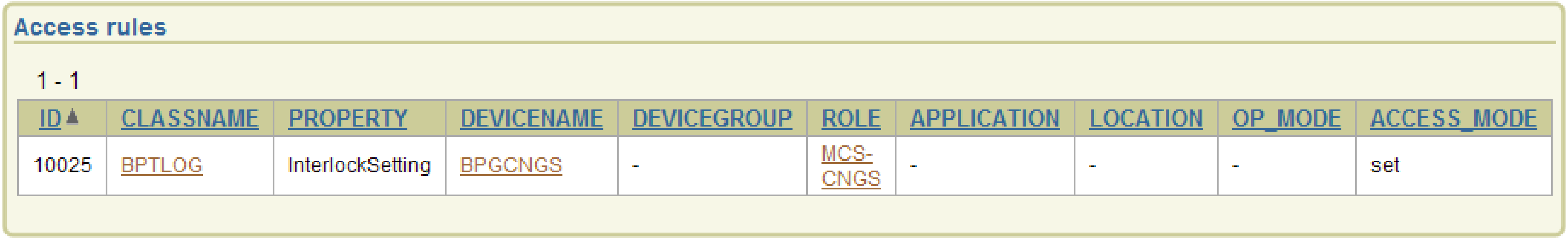
How do settings become critical settings?

- A critical role has to exist associated to the setting
  - Contact a person with the Critical-Property-Admin role


User roles

The setting is not automatically critical with a critical role!!
It needs to be set critical in LSA!!
LSA is the master. See Wojtek’s talk…

  - Define an administrator for your critical role to add the users
- Define an access rule for your equipment class, device, “critical” property (access mode: set)


Access rules

1 - 1

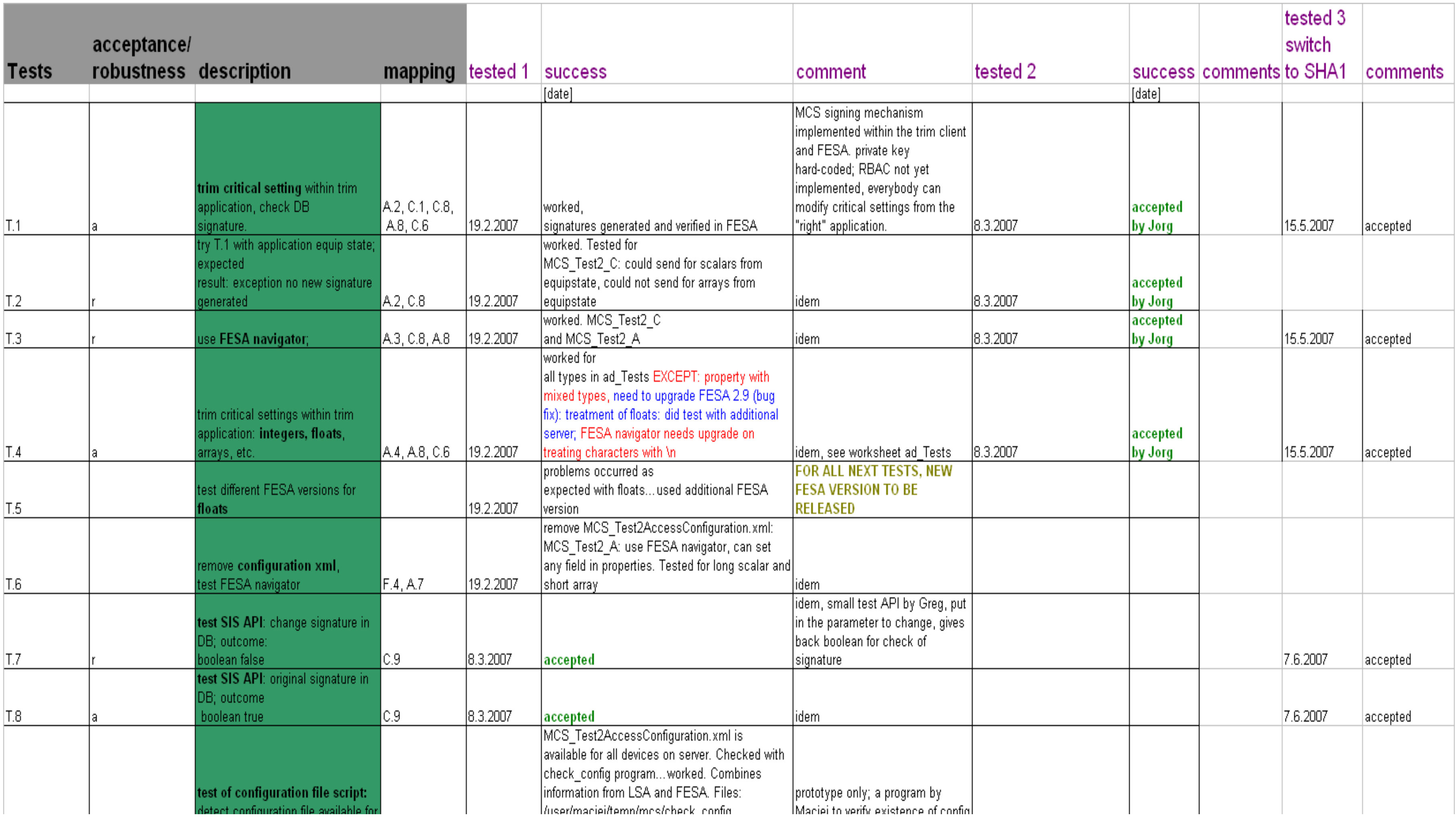
ID ▲	CLASSNAME	PROPERTY	DEVICENAME	DEVICEGROUP	ROLE	APPLICATION	LOCATION	OP_MODE	ACCESS_MODE
10025	BPTLOG	InterlockSetting	BPGCNGS	-	MCS-CNGS	-	-	-	set

Which critical settings are/will there be at LHC start-up?

Critical setting	Comment
Collimator and passive protection device limit functions	Multiplexed, actual settings and functions; FESA front-ends; read-write
LHC BLM applied tables	Non-multiplexed, matrices, FESA front-ends; read-write
LBDS XPOC references	Non-multiplexed, 22 critical multi-field (multi-type) properties per virtual device (spring server), 1 device per beam; read-write
LBDS look-up tables	Non-multiplexed, FESA front-end, read, write to DB only
Safe machine parameters	Non-multiplexed, FESA front-end; read-write
BIS configurations	Non-multiplexed, read, write to DB only
MKI injections kickers	Non-multiplexed, FESA front-end, delay, kick voltage, length; read-write
Point 6 interlocked BPMs	Non-multiplexed, FESA front-end; read-write
SPS-LHC transfer	Multiplexed/Non-multiplexed, FESA front-ends, read-write: BLMI, BPCEs, power converter current references and tolerances

MCS-Testing (1)

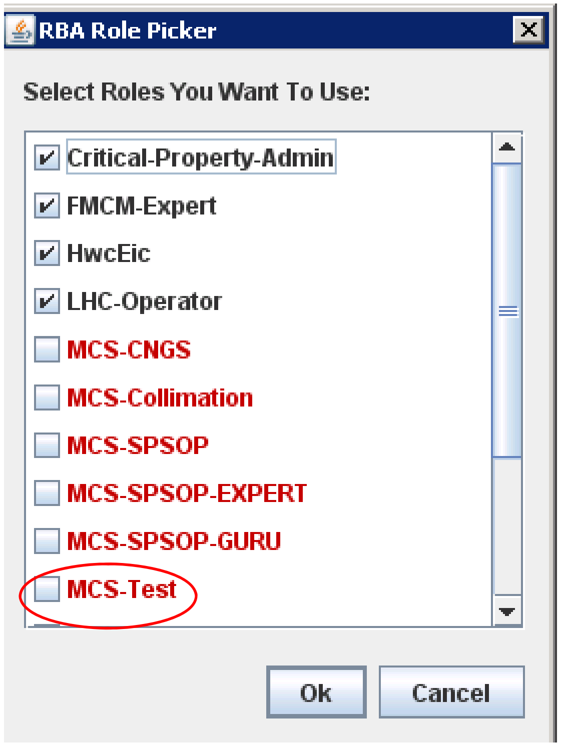
- Each feature of MCS is associated with a test. A required outcome of the test is specified.



Tests	acceptance/ robustness	description	mapping	tested 1	success	comment	tested 2	success	comments	tested 3 switch to SHA1	comments
					[date]			[date]			
T.1	a	**trim critical setting** within trim application, check DB signature.	A.2, C.1, C.8, A.8, C.6	19.2.2007	worked, signatures generated and verified in FESA	MCS signing mechanism implemented within the trim client and FESA. private key hard-coded; RBAC not yet implemented, everybody can modify critical settings from the "right" application.	8.3.2007	**accepted by Jorg**		15.5.2007	accepted
T.2	r	try T.1 with application equip state; expected result: exception no new signature generated	A.2, C.8	19.2.2007	worked. Tested for MCS_Test2_C: could send for scalars from equipstate, could not send for arrays from equipstate	idem	8.3.2007	**accepted by Jorg**			
T.3	r	use **FESA navigator**;	A.3, C.8, A.8	19.2.2007	worked. MCS_Test2_C and MCS_Test2_A	idem	8.3.2007	**accepted by Jorg**		15.5.2007	accepted
T.4	a	trim critical settings within trim application: **integers**, **floats**, arrays, etc.	A.4, A.8, C.6	19.2.2007	worked for all types in ad_Tests EXCEPT: property with mixed types, need to upgrade FESA 2.9 (bug fix): treatment of floats: did test with additional server; FESA navigator needs upgrade on treating characters with \n	idem, see worksheet ad_Tests	8.3.2007	**accepted by Jorg**		15.5.2007	accepted
T.5		test different FESA versions for **floats**		19.2.2007	problems occurred as expected with floats...used additional FESA version	**FOR ALL NEXT TESTS, NEW FESA VERSION TO BE RELEASED**					
T.6		remove **configuration xml**, test FESA navigator	F.4, A.7	19.2.2007	remove MCS_Test2AccessConfiguration.xml: MCS_Test2_A: use FESA navigator, can set any field in properties. Tested for long scalar and short array	idem					
T.7	r	**test SIS API**: change signature in DB; outcome: boolean false	C.9	8.3.2007	**accepted**	idem, small test API by Greg, put in the parameter to change, gives back boolean for check of signature				7.6.2007	accepted
T.8	a	**test SIS API**: original signature in DB; outcome boolean true	C.9	8.3.2007	**accepted**	idem				7.6.2007	accepted
		test of configuration file script: detect configuration file available for			MCS_Test2AccessConfiguration.xml is available for all devices on server. Checked with check_config program...worked. Combines information from LSA and FESA. Files: /user/maciej/temp/mcs/check_config	prototype only; a program by Maciej to verify existence of config					

MCS-Testing (2)

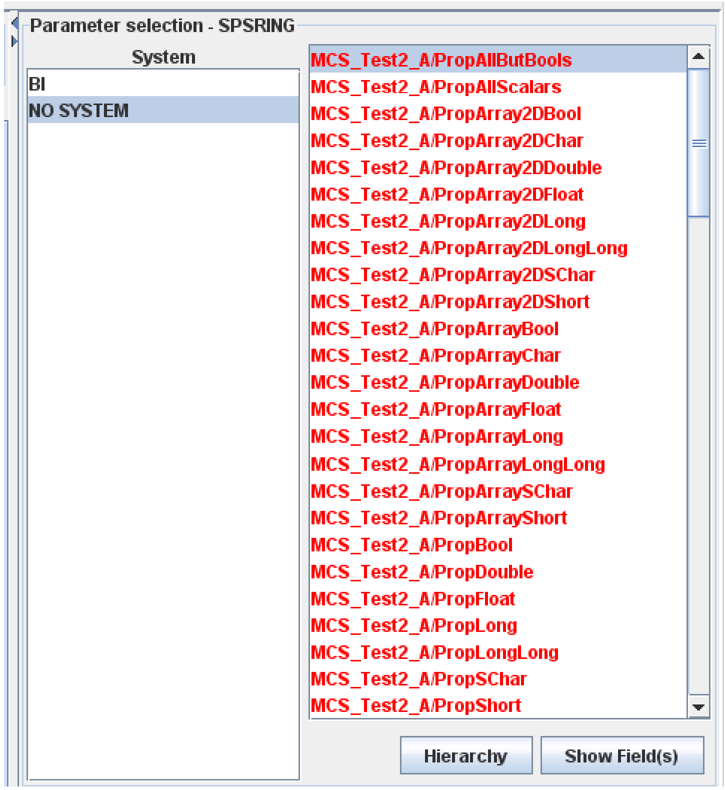
- We have test FESA devices (MCS_Test, MCS_Test2) and test critical roles
  - We test any type of data format to be signed, sent via the network and signatures verified in the DB and the front-ends (JAVA to C++)



RBA Role Picker

Select Roles You Want To Use:

- ☑ Critical-Property-Admin
- ☑ FMCM-Expert
- ☑ HwcEic
- ☑ LHC-Operator
- □ MCS-CNGS
- □ MCS-Collimation
- □ MCS-SPSOP
- □ MCS-SPSOP-EXPERT
- □ MCS-SPSOP-GURU
- □ MCS-Test



Parameter selection - SPSRING

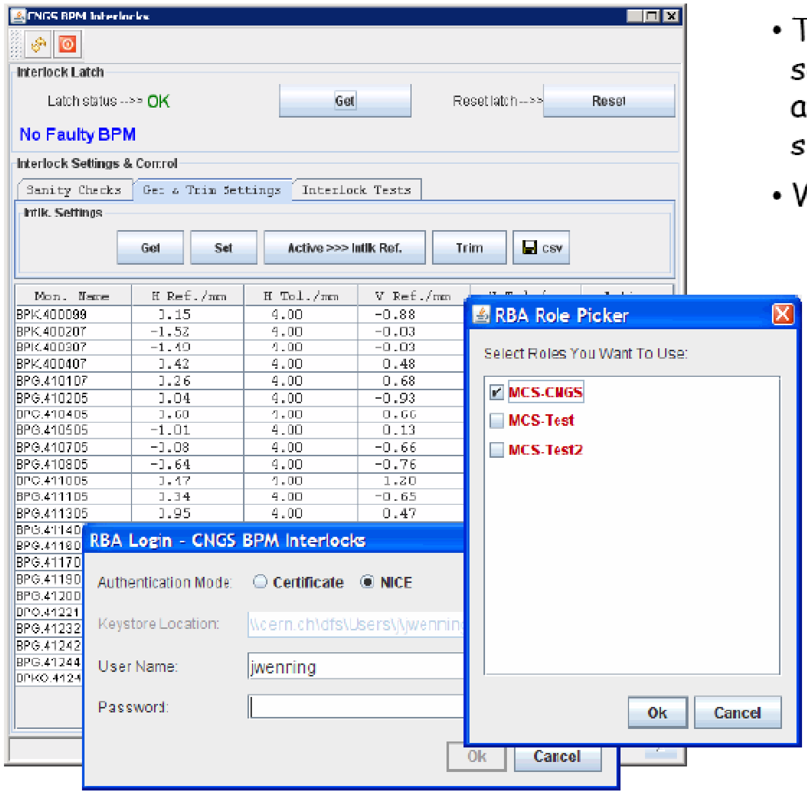
System

- BI
- NO SYSTEM

- MCS_Test2_A/PropAllButBools
- MCS_Test2_A/PropAllScalars
- MCS_Test2_A/PropArray2DBool
- MCS_Test2_A/PropArray2DChar
- MCS_Test2_A/PropArray2DDouble
- MCS_Test2_A/PropArray2DFloat
- MCS_Test2_A/PropArray2DLong
- MCS_Test2_A/PropArray2DLongLong
- MCS_Test2_A/PropArray2DSChar
- MCS_Test2_A/PropArray2DShort
- MCS_Test2_A/PropArrayBool
- MCS_Test2_A/PropArrayChar
- MCS_Test2_A/PropArrayDouble
- MCS_Test2_A/PropArrayFloat
- MCS_Test2_A/PropArrayLong
- MCS_Test2_A/PropArrayLongLong
- MCS_Test2_A/PropArraySChar
- MCS_Test2_A/PropArrayShort
- MCS_Test2_A/PropBool
- MCS_Test2_A/PropDouble
- MCS_Test2_A/PropFloat
- MCS_Test2_A/PropLong
- MCS_Test2_A/PropLongLong
- MCS_Test2_A/PropSChar
- MCS_Test2_A/PropShort

First experience with interlocked BPMs in CNGS

MCS for CNGS



CNGS BPM Interlocks

Interlock Latch

Latch status -->> OK | Get | Reset latch -->> | Reset

No Faulty BPM

Interlock Settings & Control

Sanity Checks | Get & Trim Settings | Interlock Tests

Intlk. Settings

Get | Set | Active >>> Intlk Ref. | Trim | csv

Mon. Name	H Ref./mm	H Tol./mm	V Ref./mm
BPK.400099	1.15	4.00	-0.88
BPK.400207	-1.52	4.00	-0.03
BPK.400307	-1.49	4.00	-0.03
BPK.400407	1.42	4.00	0.48
BPG.410107	1.26	4.00	0.68
BPG.410205	1.04	4.00	-0.93
DPG.410405	1.60	4.00	0.66
BPG.410505	-1.01	4.00	0.13
BPG.410705	-1.08	4.00	-0.66
BPG.410805	-1.64	4.00	-0.76
DPG.411005	1.47	4.00	1.20
BPG.411105	1.34	4.00	-0.65
BPG.411305	1.95	4.00	0.47
BPG.41140			
BPG.41180			
BPG.41170			
BPG.41190			
BPG.41200			
DPG.41221			
BPG.41232			
BPG.41242			
BPG.41244			
DPKO.4124			

RBA Login - CNGS BPM Interlocks

Authentication Mode: ○ Certificate ● NICE

Keystore Location: \\cern.ch\dfs\Users\j\jwennin

User Name: jwenring

Password:

Ok | Cancel

RBA Role Picker

Select Roles You Want To Use:

☑ MCS-CNGS

□ MCS-Test

□ MCS-Test2

Ok | Cancel

- The CNGS beam position interlock settings (references, tolerances & active status) were the first OP setting to be used with MCS. scheme.
- Worked fine after a few iteration.

J. Wenninger MPWG meeting 1Feb08

16

Documentation

- Documentation
    - For users
    - For equipment owners
    - For application developers
  - Role Based Access Control
    - http://wikis/display/LAFS/Role-Based+Access+Control
  - Management of Critical Settings
    - http://wikis/display/LSA/MCS+-+Management+of+Critical+Settings

Wojtek’s talk…