104th meeting of the

LHC Collimation Study Group

Geneva, 24th August 2009

Final implementation of RBAC for collimators

S. Redaelli, R. Assmann, A. Masi

Acknowledgments: M. Donze, G. Kruk, W. Sliwinski, M. Sobczak

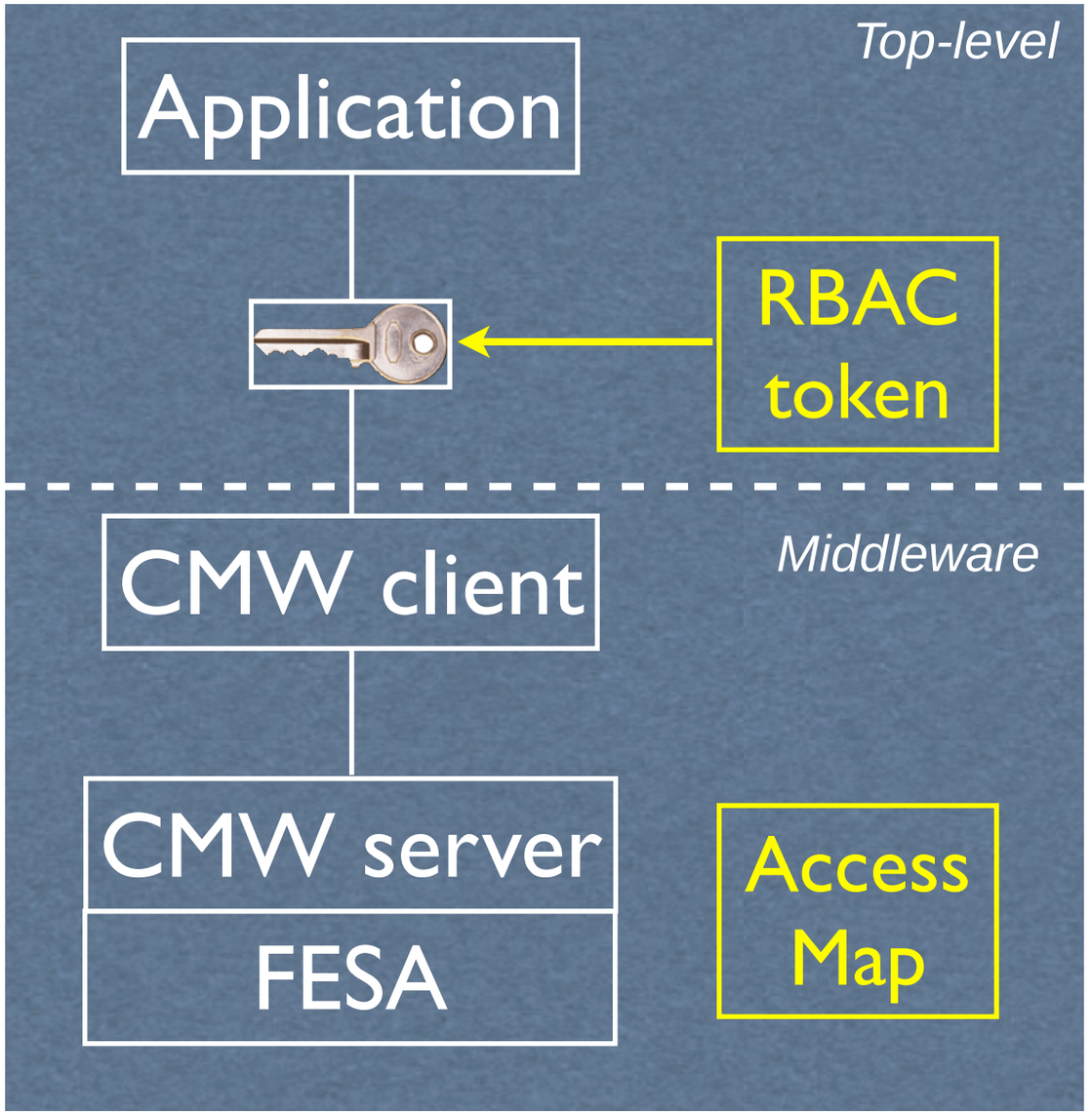
P. Charrue, V. Kain, E. Mc Crory, J. Wenninger

Outline

- **Framework**
  - RBAC in a nutshell
  - MCS in a nutshell
- **Collimation Roles&Rules**
  - Position control
  - Temperature controls
- **Implementation and tests**
- **Conclusions**

Role-Based Access Control (RBAC)

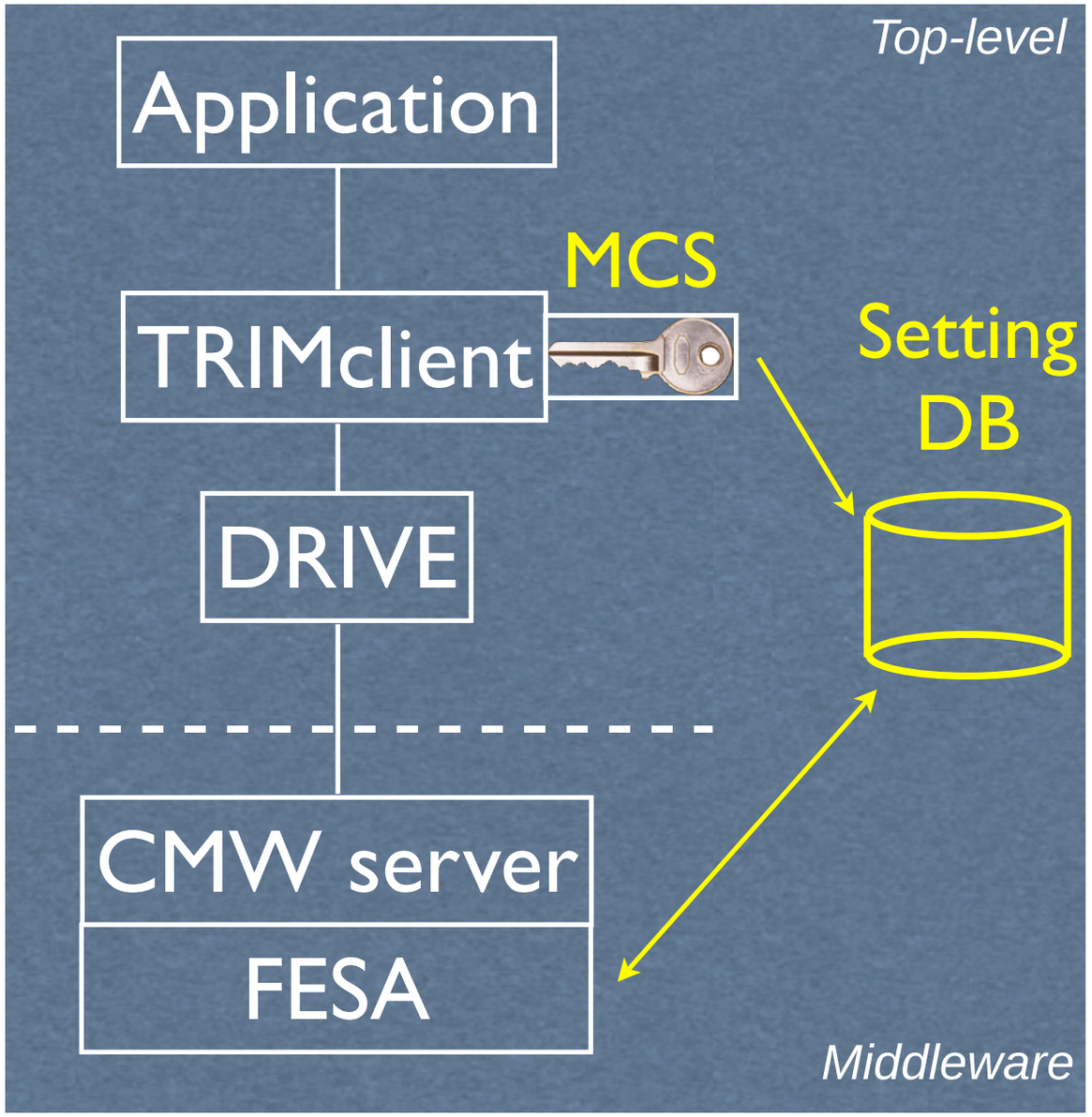
- RBAC is designed to **protect settings** of the hardware **from unauthorized users**: the access to properties and fields of the Front-Ends that control the hardware is restricted.
- Middle-ware:
  An “access map” must be defined for all setting properties. It is used to define **ROLES**/**RULES** for different **LOCATION**/**OP_MODE**.
  Certain roles are assigned to users.
  Ex.: Ralph has the Collimator Expert role that allows him to “set” the properties x, y, z from his office during the shutdown and only from the CCC in the operational mode.
- Client applications:
  Must integrate with RBAC infrastructure and pass a “token” with the user’s credentials to CMW server, before accessing equipment (e.g. FESA).
- Access maps defined by HW owners + OP
- RBAC tested in STRICT MODE since mid-July



References:
W. Sliwinski, http://wikis/display/ABCO/TC-165+02.07.2009
P. Charrue, at the LHCWG of Aug. 4th
R. Alemany at the LHCCWG of June 23rd

Management of Critical Settings (MCS)

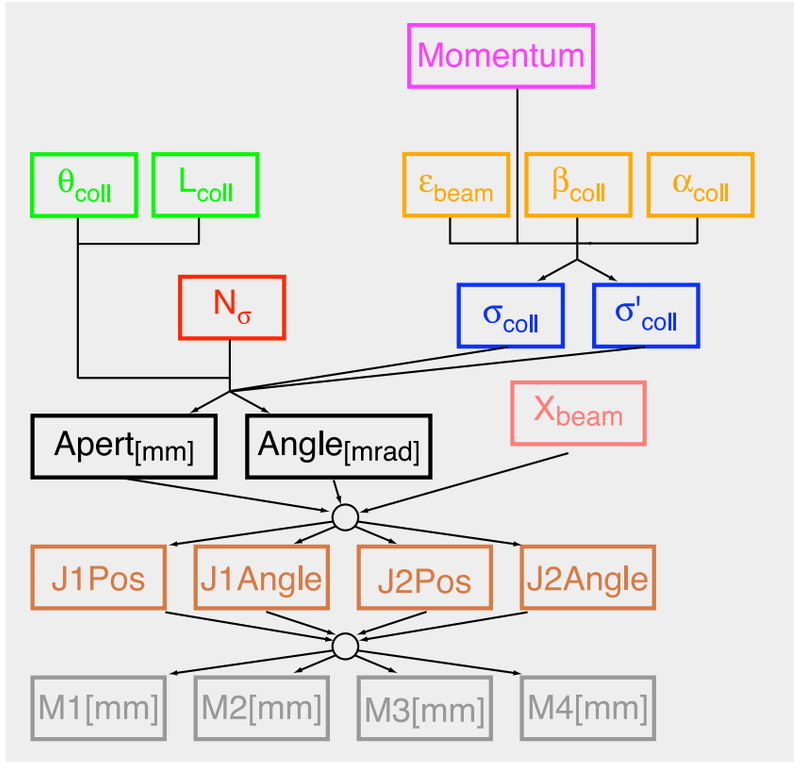
- Further protection of interlock settings: in addition to the authentication, MCS is designed to **assure consistency of settings**.
  Settings are **digitally** signed.
- Functionality is built into the LSA trim package:
  Signature computed for the parameters flagged as “critical” and stored in the DB with the settings; then checked at front-ends.
- Authentication is done by RBAC (an appropriate “MCS-role” has to be defined)
- Remark (subtlety):
  During standard operator, LHCOP must be able to “load”/“drive” critical settings but is **not** authorized to change their references in the database!
  LHCOP does not have critical roles BUT has the RBAC authority to change critical properties handled by MCS!
  Careful: if the operators loads the WRONG cycle, MCS can be completely by-passed!!!

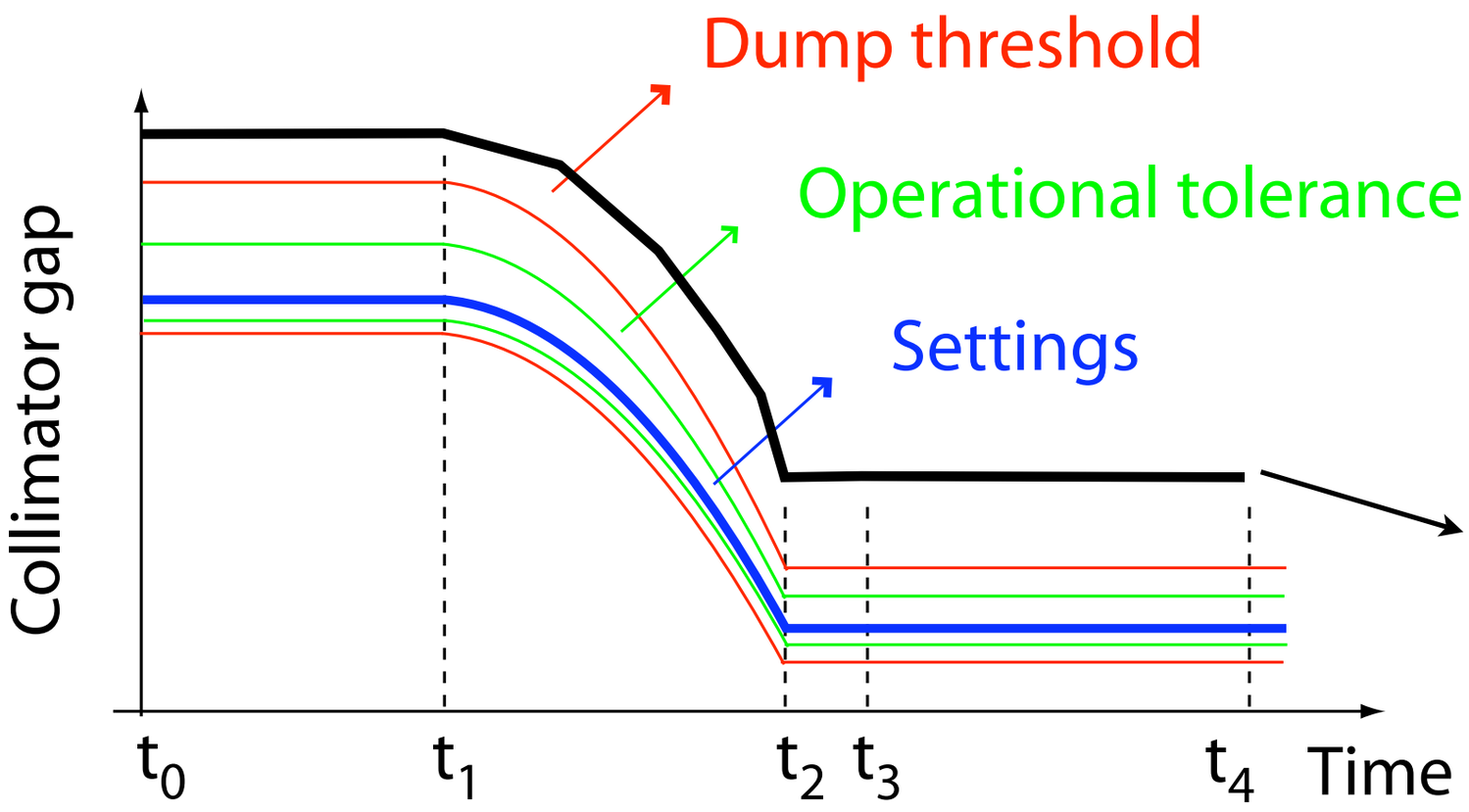


Refs.: V. Kain at the LTC of May 24th, 2006.

Critical properties for positioning

- Collimator parameters for standard operation:
  - Position settings
  - Software triggers to start movements
  - Reset of errors/warnings
  - Disarm, stop commands
- Collimator critical settings: all interlock thresholds
  - Position/gap limits versus time (functions)
  - Constant position/gap limits (discrete)
  - Gap limits versus energy (functions)
  - Temperature thresholds





1 collimator =
4 motors settings +
24 position limits +
5 temperature thresholds

=> Need an efficient handling of all the functions! ! !

Energy (beta*) functions (gaps only)

Collimators: Roles and Rules

Monitoring: No restriction

	Role	Rights	Location / OP mode
STI	**STI-LHC-USER**	Read-only: no settings allowed.	Everywhere/No-OP MODE Everywhere/OP MODE
	STI-LHC-EXPERT	Expert and operator settings allowed but no critical settings (MCS) and no modification of the LVDTs calibration tables. Can move the fifth motor axis for all collimators.	Everywhere/No-OP MODE CCC / OP MODE
	STI-LHC-PIQUET	Allowed all the expert and operator settings without beam, including bypassing MCS (interlock thresholds) at low level and updating the calibration table.	Everywhere / OP MODE
Operation of the system	**LHC-Operator**	All operator settings allowed including SENDING critical settings to the low level. Automatic collimator tuning and the update of the motor controller on the LVDT values are NOT allowed. Can not change critical settings in the setting database, can drive pre-defined settings. Can move the fifth motor axis only for the 6 two-in-one colls.	Everywhere/No-OP MODE CCC / OP MODE
	LHC-COLL-EXPERT	All operator settings allowed including SENDING critical settings to the low level. Automatic collimator tuning and the update of the motor controller on the LVDT values are allowed. Can not change critical settings in the setting database, but can drive them. Can move the fifth motor axis only for the 6 two-in-one colls.	Everywhere/No-OP MODE CCC / OP MODE
Critical settings	**MCS-Collimation**	Can generate and change the critical settings, namely discrete and time-dependent interlock thresholds and gap limits versus energy. For operational convenience, the MCS role must also be able to change the setting properties with the same role as the LHC-COLL-EXPERT.	Everywhere/No-OP MODE CCC / OP MODE

REMARK: only operational roles can changes settings with beam in the machine!

Roles and people

Present configuration for operational roles

LHC-Operator - LHCOP

LHC-COLL-EXPERT - C. Bracco, R. Assmann, A. Rossi, S. Redaelli, D. Wollmann

MCS-Collimation - R. Assmann, S. Redaelli

Cleaning and protection are fully coupled systems. Anybody who can change the settings must take responsibility for the whole system.

Additional collimator operators and collimator operator experts will be added (for example from TE/ABT), under the condition that they assume responsibility for the safety of the full system.

This needs to be discussed with the colleagues of injection and dump projects.

Operational “expert” roles can be different for different systems (TCDQ, Roman pots, ...).

Temperature controls

- The collimator temperature survey system consist of approximately **500 *individually* interlocked** temperature sensors (4-5 per collimator)
- For each sensor, we defined interlock (dump) limits and warning (alarm) limits.
- The controls architecture is built on PVSS
- Interlock limits for the beam permit are hard-coded in the system
- Expert operators can change the alarm limits without effect on the HW interlock
- No need for RBAC and/or MCS handling for the moment
  [BUT this is being implemented in PVSS and we can profit of it if needed!]

Status and plans

Timeline for test in 2009:

March : Systematic MCS tests started; first issues identified.

End of June : Full deployment of RBAC access map at bld. 252 (surface)
Validation with a test device to avoid perturbations of the HWC

Mid-July : Validation of all CCC applications and FESA layout; identified some issues and required improvements for the access map.

Today : Final validation of access map, start deployment for full system

Aug. 31st : Start global remote system tests in the tunnel with STRICT mode

Solved implementation issues:

RBAC : - Minor issues with FESA version 2.9, needed some patches
- Needed dedicate implementation for *multiple RBAC integrator*

MCS : - Initial problem with TRIM functions (mis-match with FESA 2D arrays)
- Problem with “transactionID” field, used to compute digital signature

Time consuming because we had to wait for a FESA release...

- Needed to change the 2008 interface for energy thresholds

Property with 3x1D arrays had to be changed to 2x2D

- Improvement of collimator hardware commands to handle signature.

TODO list of what is not yet tested:

- Copy of critical settings and settings verification in LSA
- Generation of critical settings from files

Conclusions

- **The RBAC/MCS implementation for collimators is well advanced**

  Access map deployed on a test device and thorough tests performed

- **A number of issues were found and solved**

  Less “transparent” than initially foreseen... but good support from CO colleagues.

- **Still some checks missing** (expected to be completed within ~2weeks)

  Verify implementation of new hardware commands for critical settings

  MCS setting copy and checks; generation of critical settings from file.

- **The assignment of users to critical roles&rules must be finalized with the injection and dump colleagues**

- **The next challenge is to start the remote system commissioning with RBAC in STRICT mode**

  Find as soon as possible other possible issues

  Assess the operability of the system with full protection in place

Reserve slides

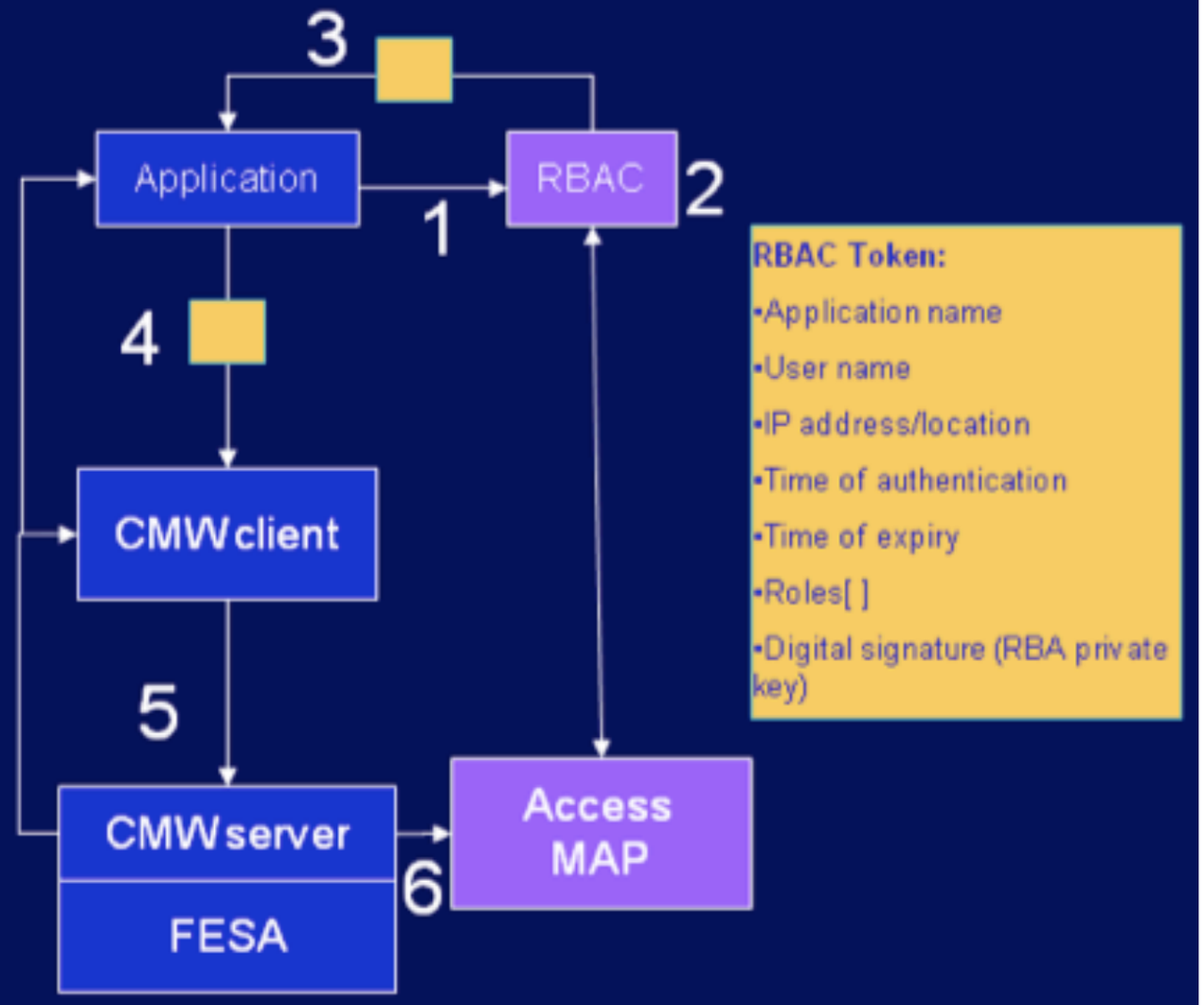
High Level Design

Authentication:

1. User requests to be authenticated.
2. RBAC authenticates user via NICE user name and password or location
3. RBA returns token to Application

Authorization:

4. Application sends token to CMW when connecting.
5. CMW/FE verifies token signature once, and uses the credentials for every subsequent request
6. CMW checks access map for role, location, application, mode



From W. Sliwinski's presentation available at http://wikis/display/ABCO/TC-165+02.07.2009