

SECAM application: a concrete example in Methodology 2

Loïc HABERMACHER, Isabelle KRAEMER – Orange
3GPP SA3#71 meeting (8th – 12th of April 2013)



How it could work

1. Preliminary work for each product class
 - define threats applying
 - define suitable attacker model
 - take into account dependencies to environment
2. SAS building block writing, according to step1
 - bunch of security requirements
 - grouped by topics

What it could look like for an evaluator

eNB SAS

Work hypothesis

- eNB's attacker model
- eNB's threats
- eNB's environment

↓

Necessary BB

- building block 1
- building block 2
- ...



MME SAS

Work hypothesis

- MME's attacker model
- MME's threats
- MME's environment

↓

Necessary BB

- building block 1
- building block 4
- ...



Building blocks

- building block 1
- building block 2
- building block 3
- building block 4
- building block 5
- building block 6
- ...



The admin function

A CONCRETE EXAMPLE

1. define threats

- Threats
 - Theft of admin service – use cases
 - Theft of admin credentials
 - Guessing of admin credentials
 - Theft of admin session
 - Etc...
 - ...

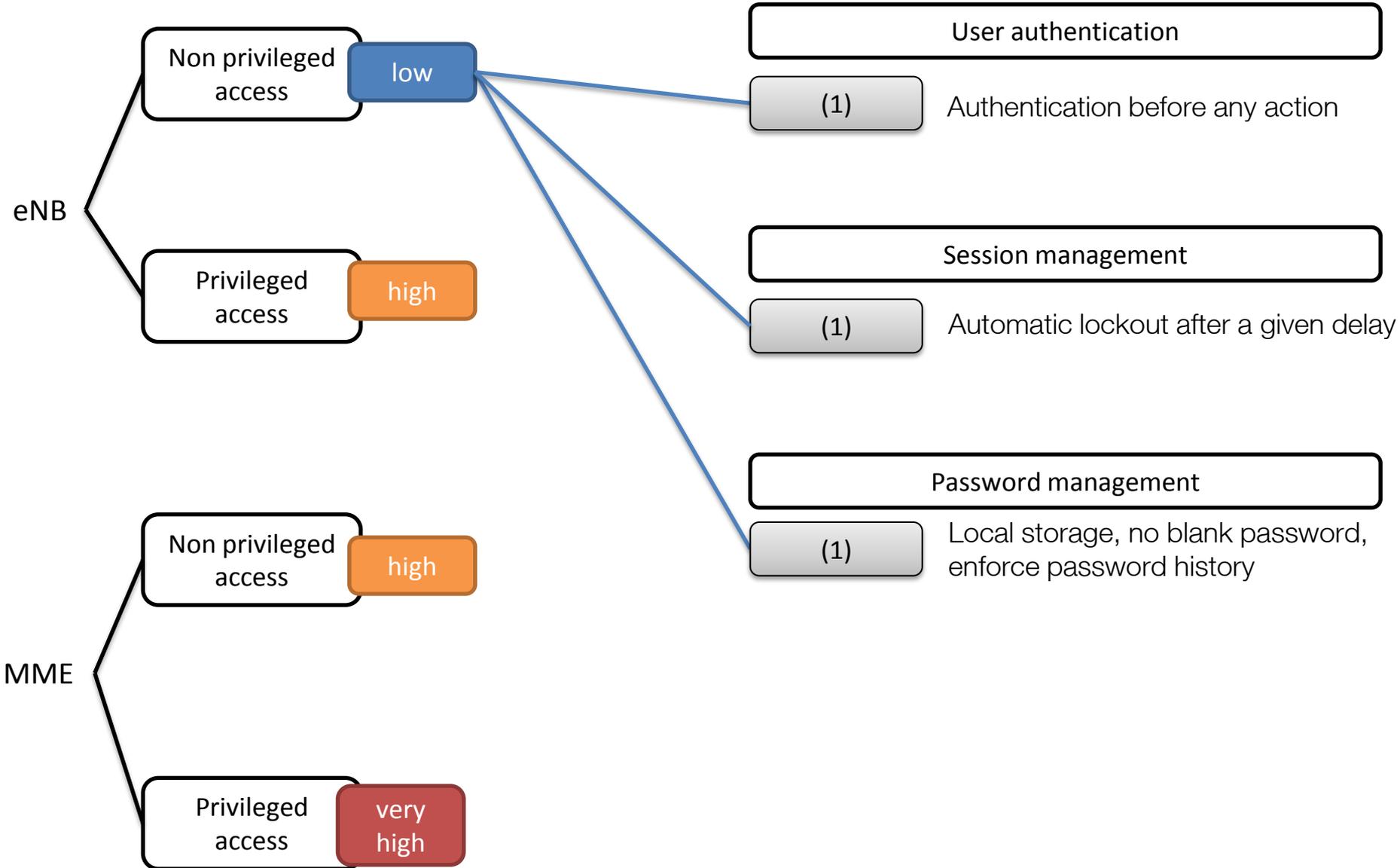
2. define attacker model

	eNB	MME
Privileged admin access <i>(installation, upgrade, access to all files)</i>	motivation/impact: high	motivation/impact: very high
Non-privileged admin access <i>(configuration, few files accessible)</i>	motivation/impact: low	motivation/impact: high

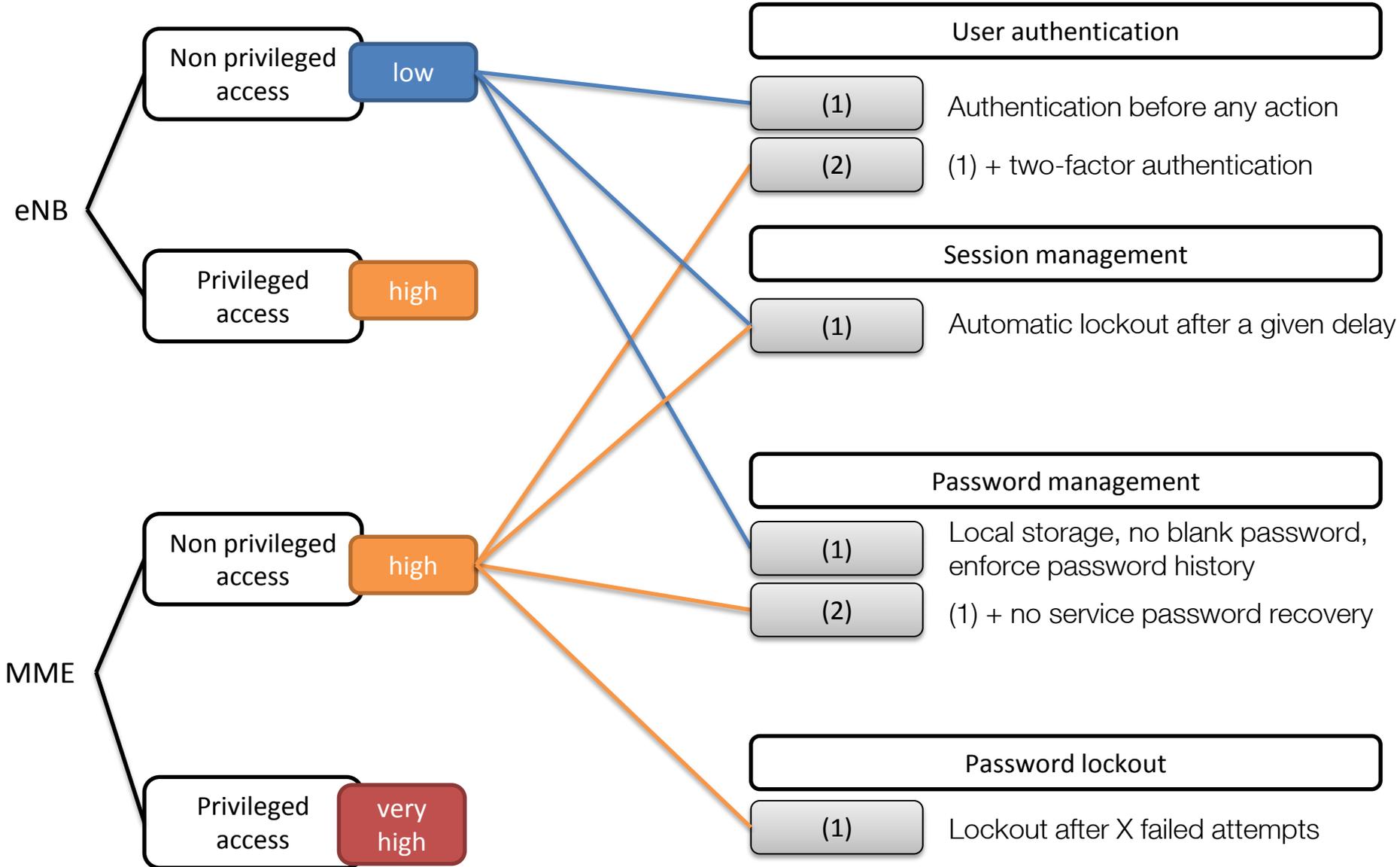
3. consider environment

- Security measures to achieve a given security level depend on assumptions made on the environment
 - Security can be partially taken care of if by an assumption that this network product class, as far as SECAM evaluations are concerned, will be deployed in a secure physical location
- Examples
 - eNB assumed to be easily accessible and thus considered exposed in SECAM evaluations
 - MME assumed to be in a secure location in SECAM evaluations
 - ⇒ security measures will take this exposure into account

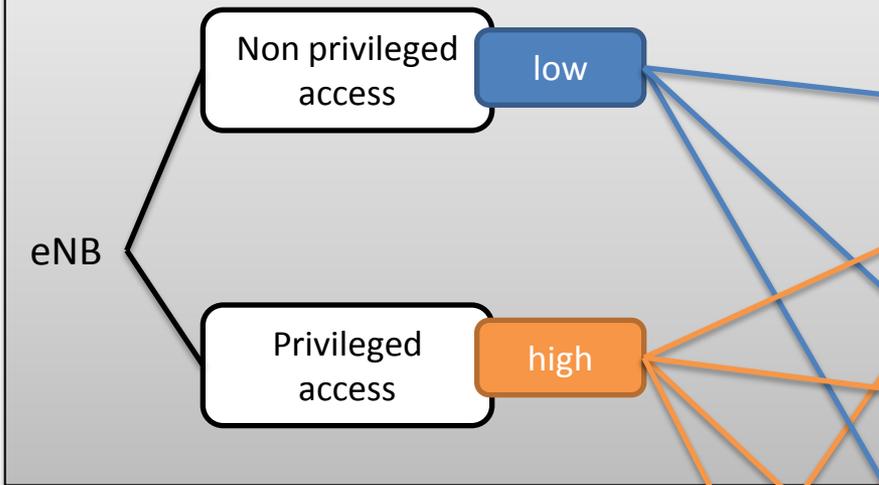
4. define building blocks



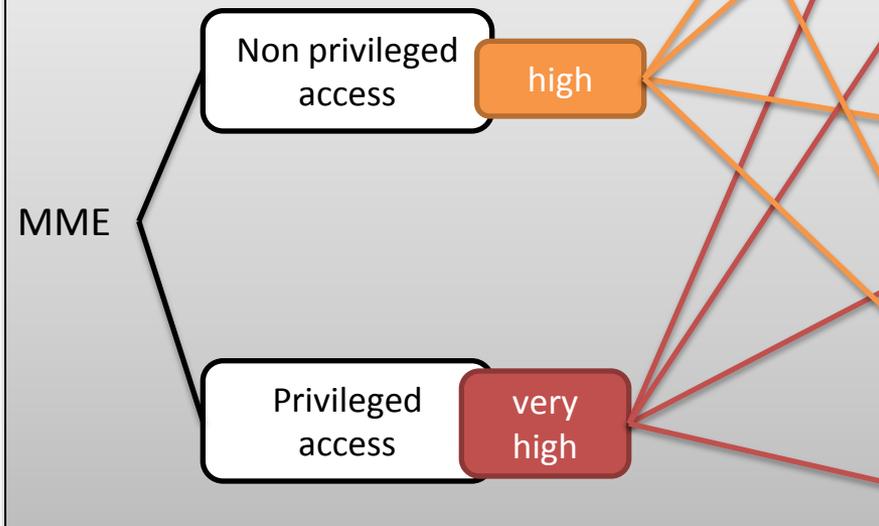
4. define building blocks



eNB SAS



MME SAS



BUILDING BLOCK DOCUMENT

User authentication

(1)

Authentication before any action

(2)

(1) + two-factor authentication

Session management

(1)

Automatic lockout after a given delay

(2)

(1) + re-authentication for each relevant security function

Password management

(1)

Local storage, no blank password, enforce password history

(2)

(1) + no service password recovery

(3)

(2) + external authentication server + enforce strong password

Password lockout

(1)

Lockout after X failed attempts

(2)

(1) + automatic configuration deletion

EVALUATION

Advantages

	eNB	MME
Topic: the admin function		
Topic: need for traffic segregation		

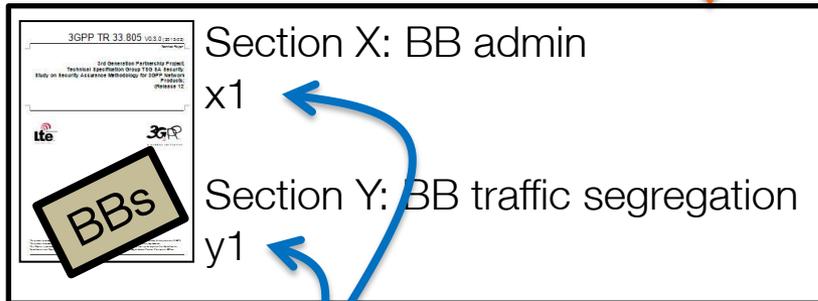
- Let's assume we need to address 2 topics:
 - discussion on admin services
 - given attacker model & environment, assess threat level
 - consequently, define suitable BB
 - discussion on traffic segregation
 - idem
- No time dependency between different topics discussed

Advantages

	eNB	MME
Topic: the admin function		
Topic: needed traffic segregation		

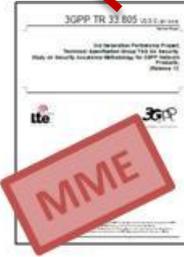
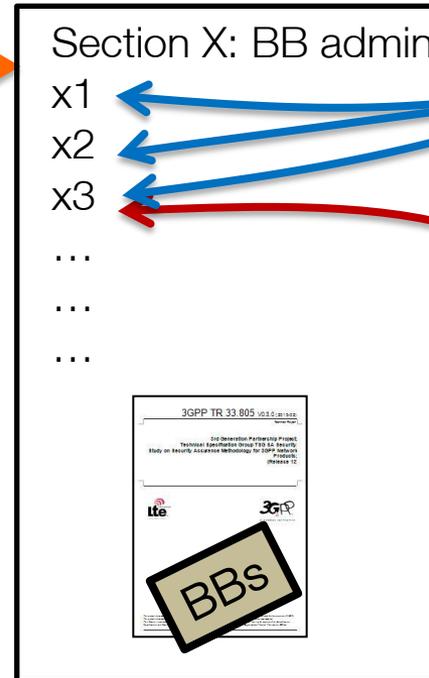
possible to work at the same time:

- on *different* subjects
- for the *same* network product class



Advantages

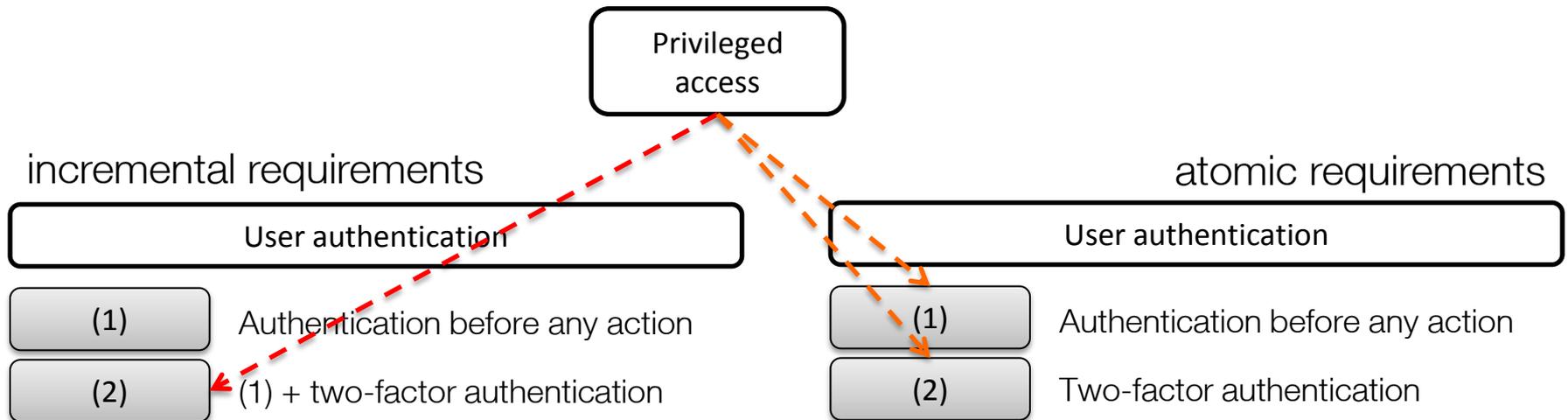
	eNB	MME
Topic: the admin function		
Topic: needed traffic segregation		



- possible to work at the same time
- on *same* subject
- for *different* network product classes

Open issues

- Maintenance needed: potentially lots of (irrelevant) updates
 - a reference for a requirement (X.Y.Z.A.B) in BB changes => all related SAS have to be updated (similar issue in any 3GPP document however)
- Inheritance for BB needed?
 - atomic requirements vs. incremental requirements



- **No need to reach an agreement on these questions now as both ways are workable for the normative phase**

Concrete proposal

- Discuss this contribution
 - questions, remarks, etc...
- Either for SA3#71
 - add the example of implementation of Methodology 2 for the admin functions of an eNB and an MME network product classes (section A.2)
- Or for SA3#72 if major changes are required and not doable during SA3#71
 - Come back to SA3#72 with an updated contribution

thanks

Orange, the Orange mark and any other Orange product or service names referred to in this material are trade marks of Orange Brand Services Limited.

Orange restricted.

