brightsight®

your partner in security approval

Peter van Swieten
+ 31 15 269 2500
swieten@brightsight.com
www.brightsight.com

Experience with CC 3.1, Class ALC (Life Cycle Support) evaluation

Contents

Who am I?

Common Criteria evaluator mainly involved in CC evaluation of

- IC-Card

- Pin Entry Device (PED)



⇨ High level of security assurance EAL4+ (AVA_VLA.3/4 or AVA_VAN.4/5)
This presentation focuses on high assurance levels and complex processes

ALC introduction

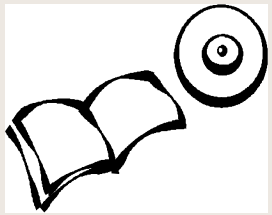
- Position of ALC within a CC evaluation
- ALC classes
- The challenges for the ALC evaluator

ALC introduction,
The position of ALC within a CC evaluation

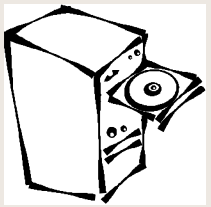
Life-cycle support (ALC)

Security Target evaluation (ASE)

Development (ADV) with FSP, TDS, IMP, ARC



Guidance (AGD)



Tests (ATE)
Vulnerability Assessment (AVA_VAN)

ALC classes (1)

ALC - Life-Cycle support (According to CC 3.1)

ALC_CMC	CM capabilities
ALC_CMS	CM scope
ALC_DEL	Delivery
ALC_DVS	Development security
ALC_FLR	Flaw remediation (optional)
ALC_LCD	Life cycle definition
ALC_TAT	Tools and techniques

ALC classes (2)

- Version management system related: (ALC_CMC & ALC_CMS)
- Shipment related (ALC_DEL & ALC_DVS)
- Logical & physical site security related (ALC_DVS)
- Security flaws handling (ALC_FLR)
- Development and maintenance processes related (ALC_LCD)
- Tools & Techniques (ALC_TAT)

The challenges for the ALC evaluator

Obtaining and reporting the overview

Determining whether the security measures are sufficient

Obtaining and reporting the overview (1)

Expected actions in creation of a TOE:

- Design/development
- Production
- Shipment to customer

Obtaining and reporting the overview (2)

Three realistic cases ranging from simple to difficult.

1. A TOE (e.g. a software product) that is developed, produced and shipped in one site.

2. A TOE (e.g. PED) with 2 development sites (SW+HW), 1 production site and 2 shipment site

3. A TOE (e.g. IC-Card) with 3 development sites, 3 production sites, 1 shipment site.

The following sheets show the overview for case 3

Obtaining and reporting the overview (3)

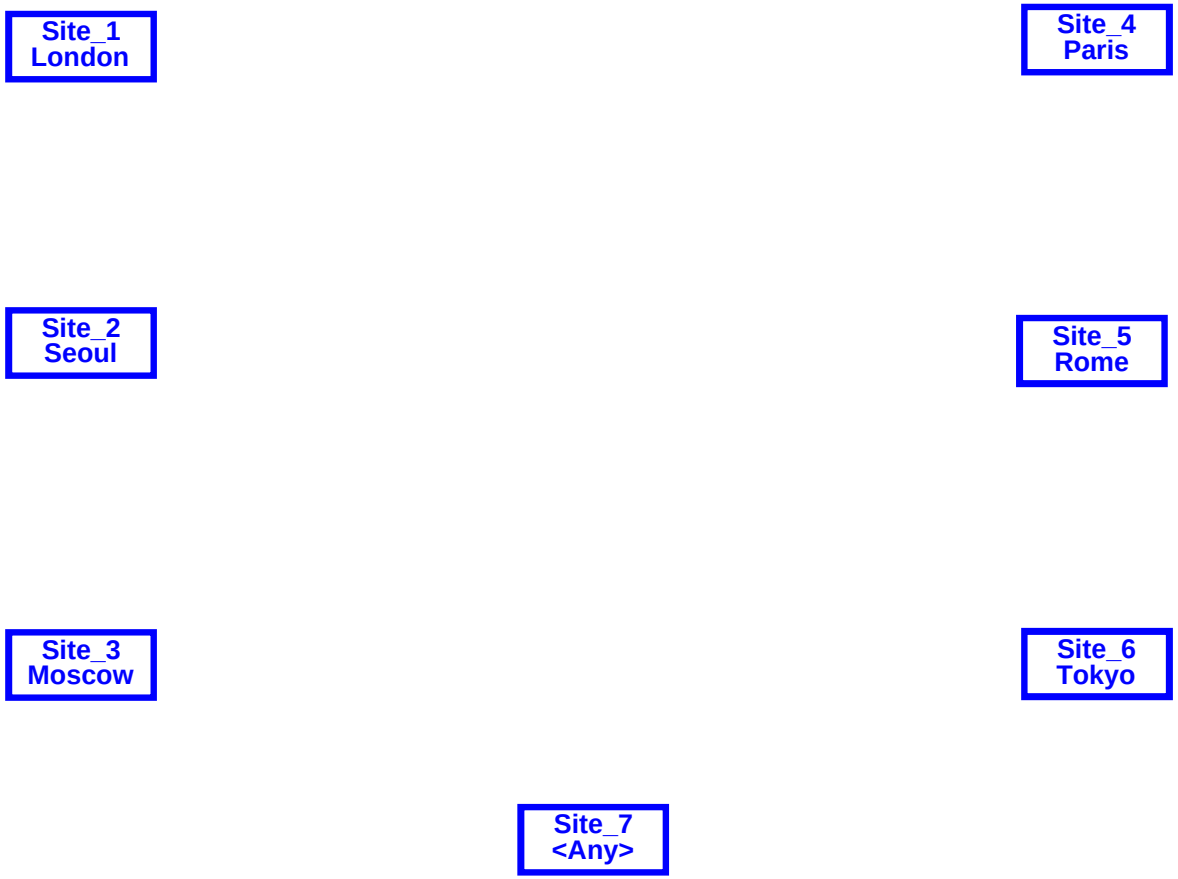
The evaluator task is to check each of the ALC requirements.

- The input: The ALC documentation.
- The task: Performing all ALC work units.
- The output: A report showing the result the ALC work units such that it is understandable for the scheme.

The difficulty for the evaluator: Have to start from scratch while the input typically consists of at least 1 document for each site:

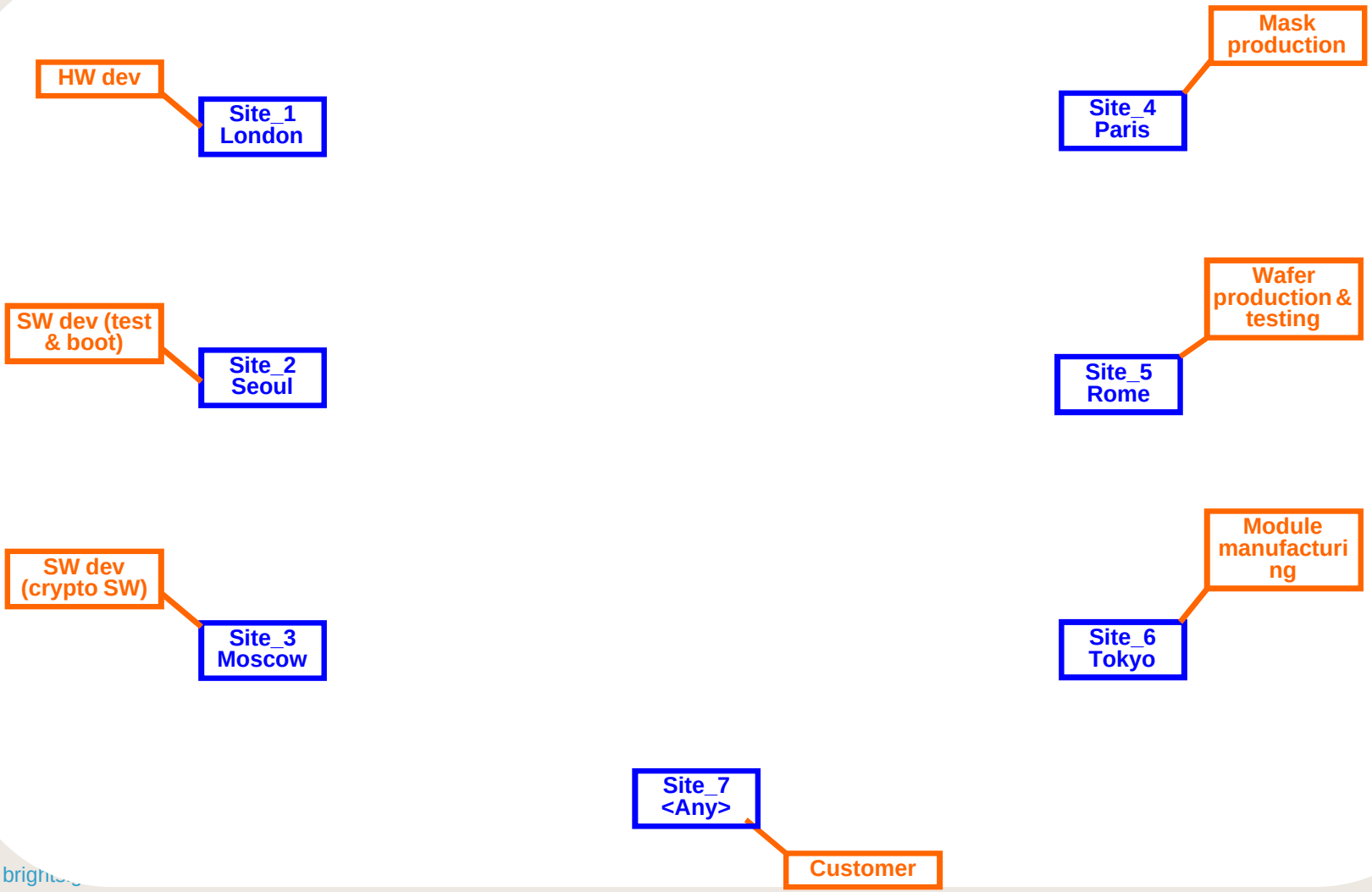
Obtaining and reporting the overview (4)

Step 1: Which sites are involved? (Example: IC-card developer)



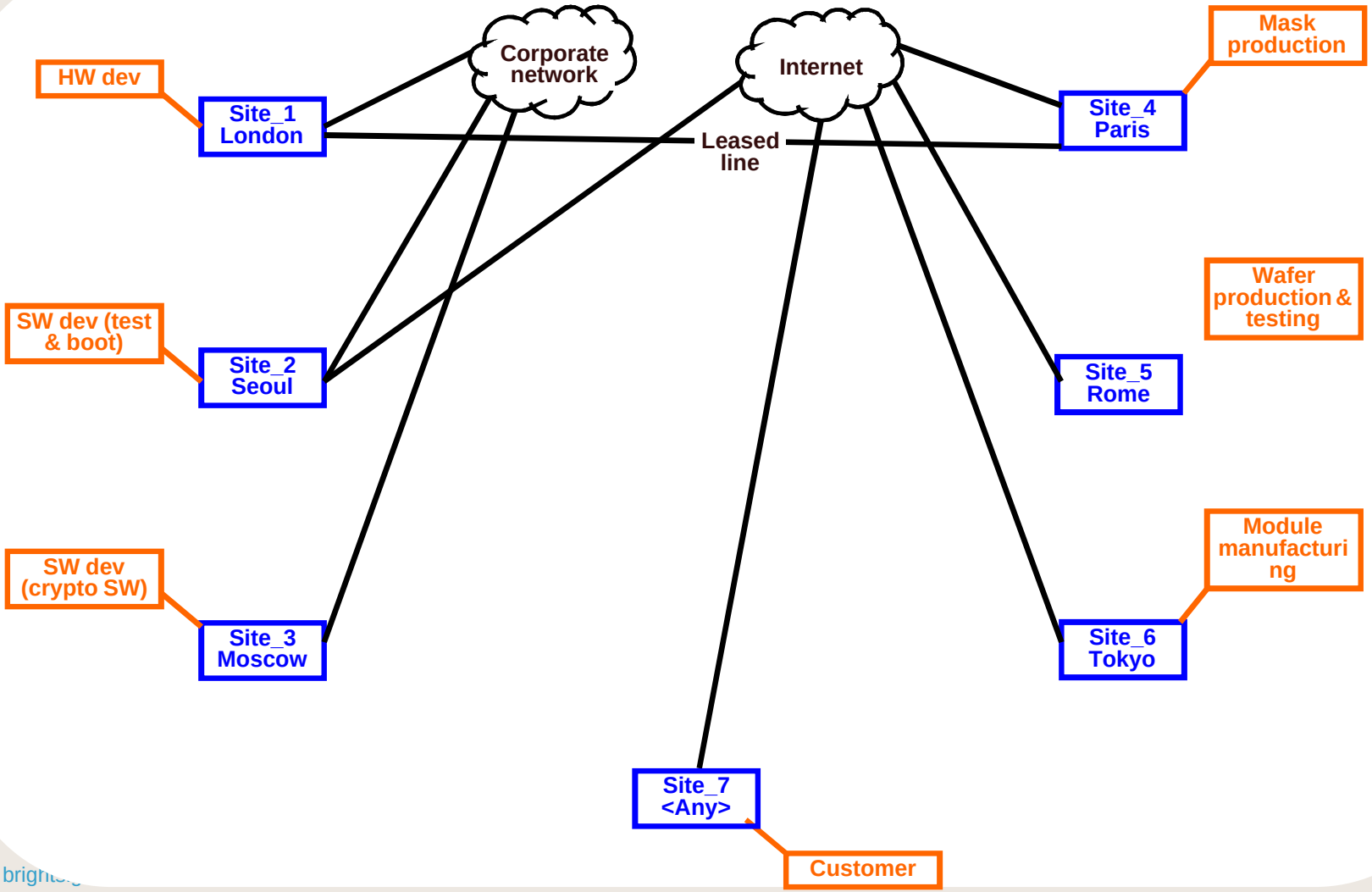
Obtaining and reporting the overview (5)

Step 2: What do these sites do? (Example: IC-card developer)



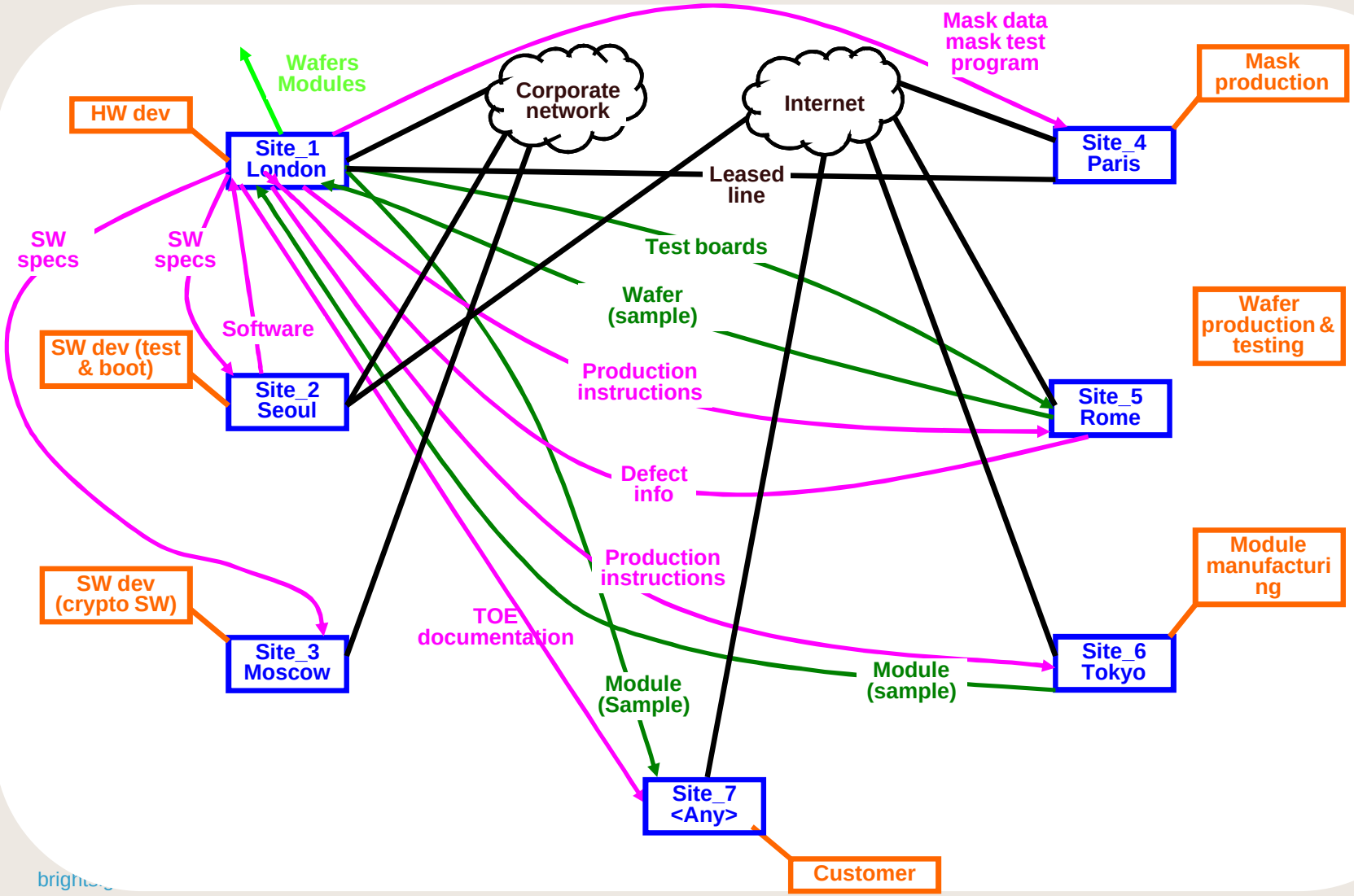
Obtaining and reporting the overview (6)

Step 3: What IT networks are involved? (Example: IC-card developer)



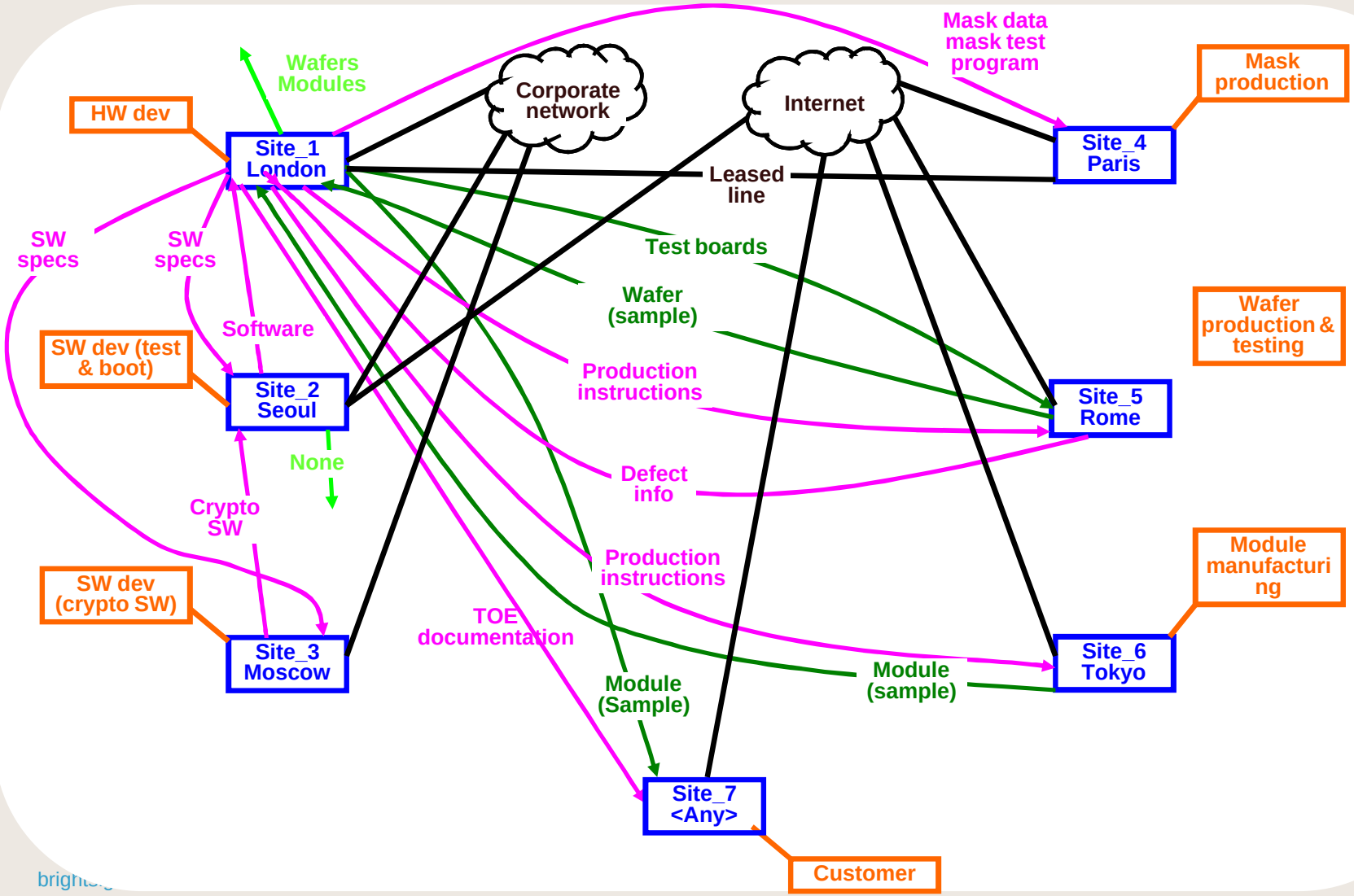
Obtaining and reporting the overview (7)

Step 4a: For site 1 add shipment and disposal (Example: IC-card developer)



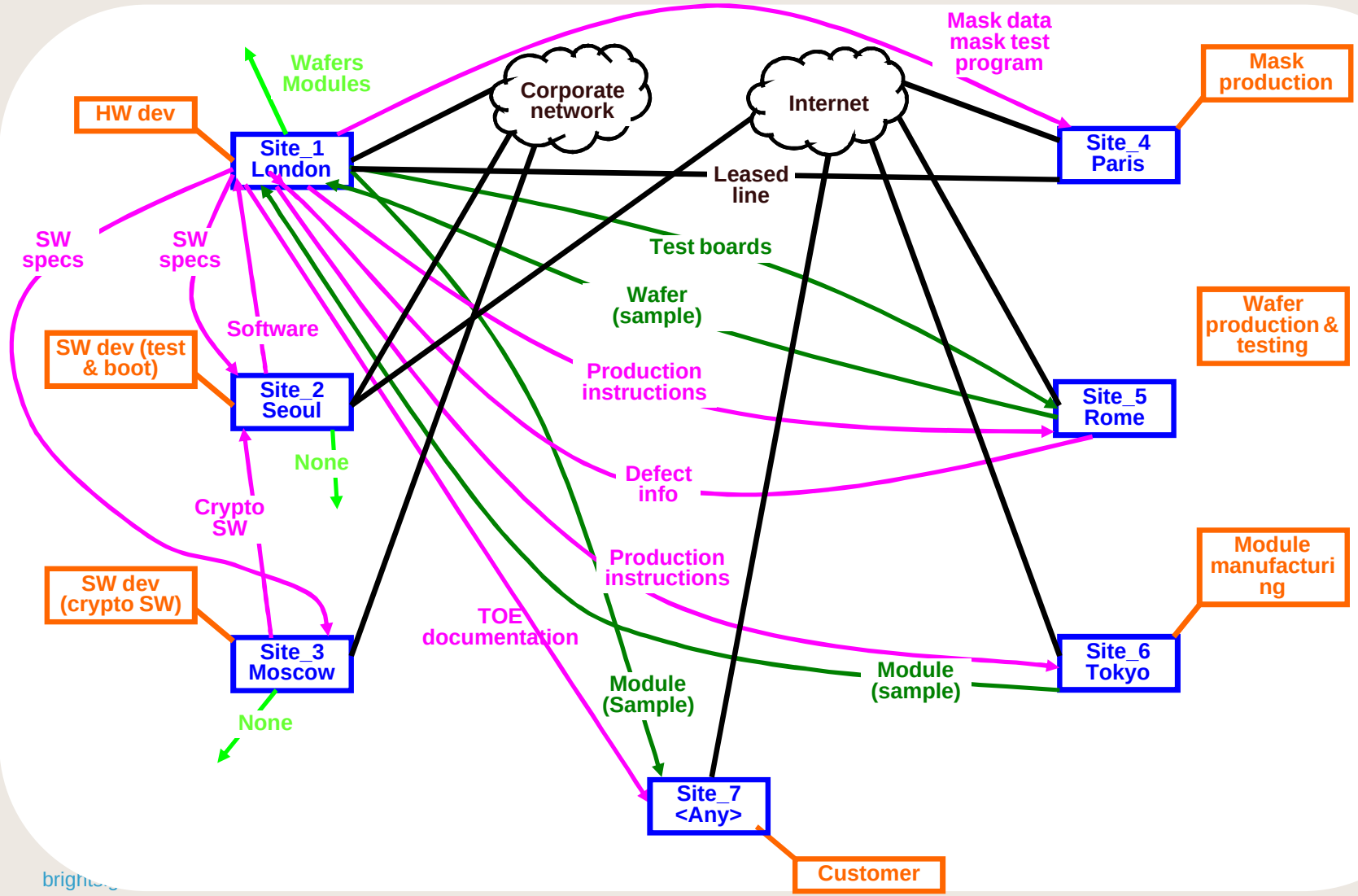
Obtaining and reporting the overview (8)

Step 4b: For site 2 add (and check consistency of) shipment and disposal (Example: IC-card developer)



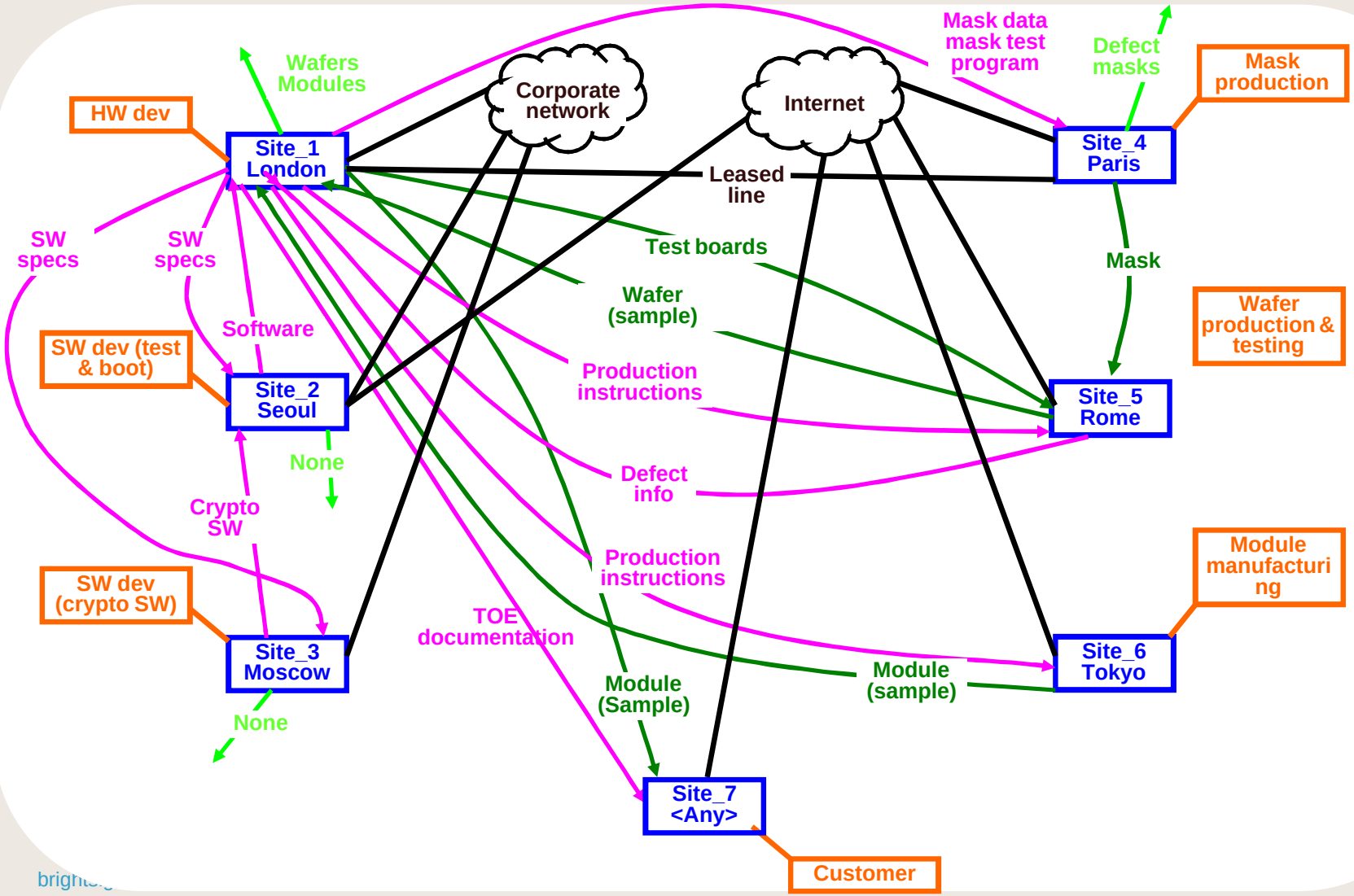
Obtaining and reporting the overview (9)

Step 4c: For site 3 add (and check consistency of) shipment and disposal (Example: IC-card developer)



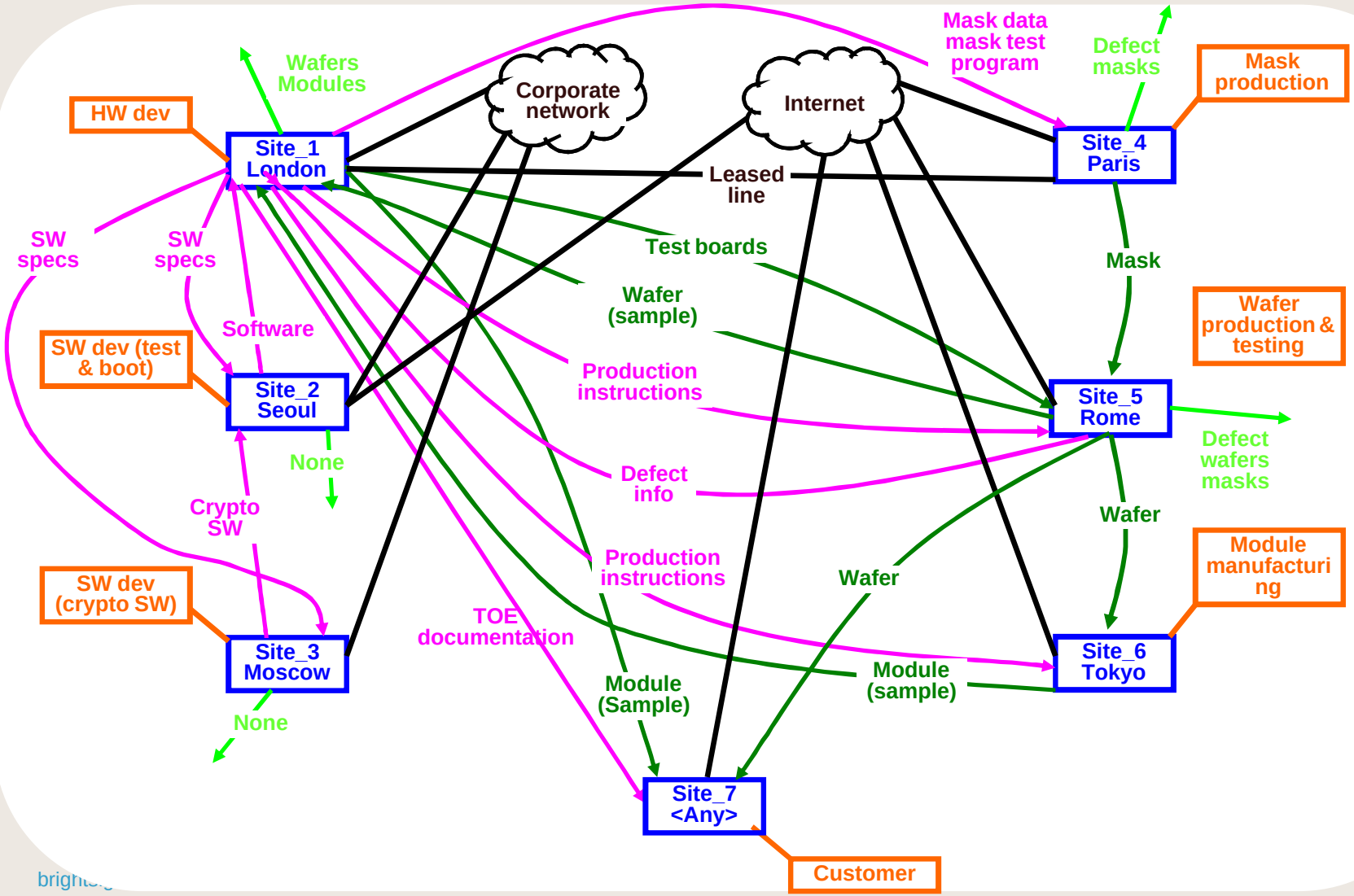
Obtaining and reporting the overview (10)

Step 4d: For site 4 add (and check consistency of) shipment and disposal (Example: IC-card developer)



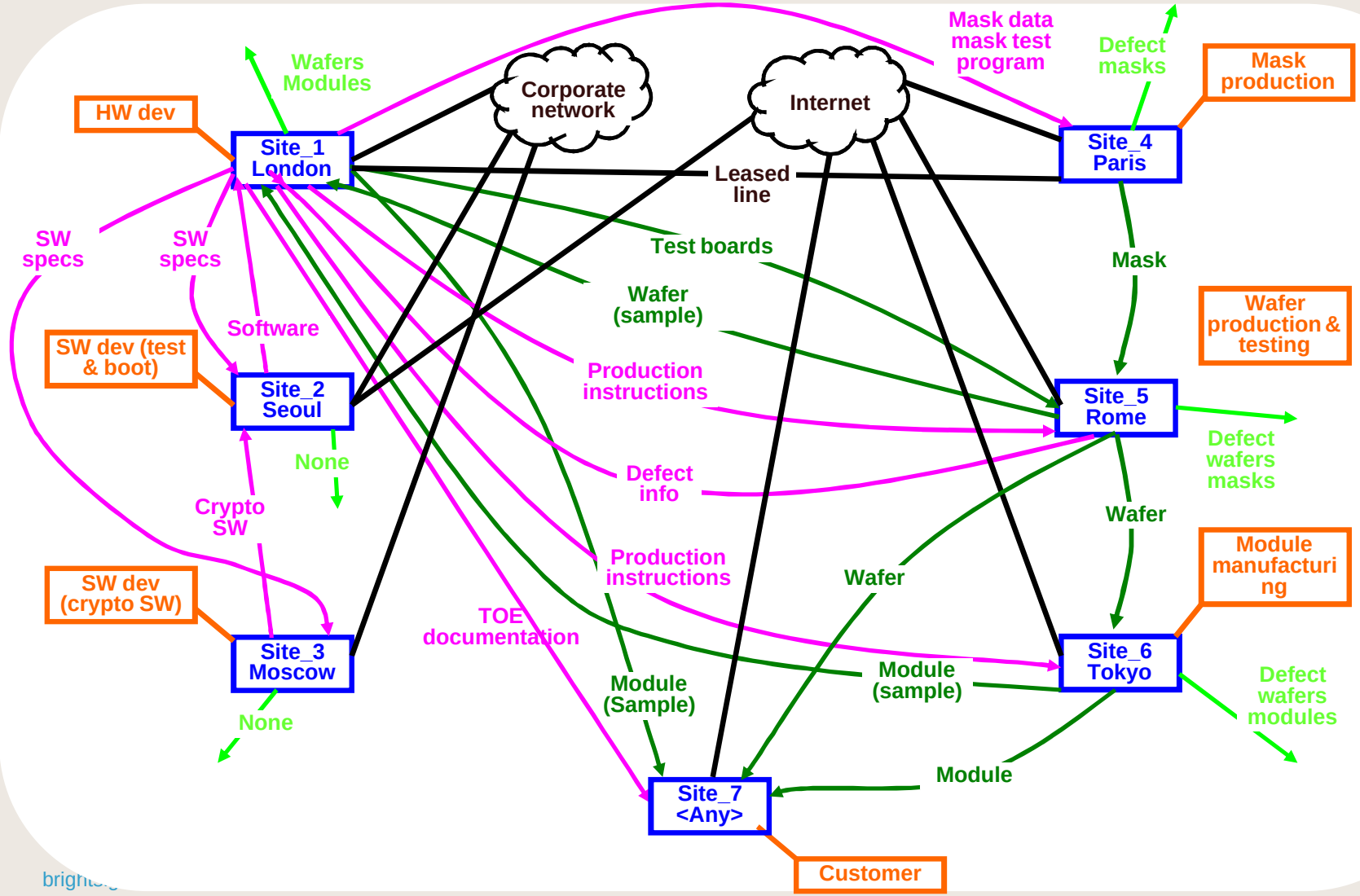
Obtaining and reporting the overview (11)

Step 4e: For site 5 add (and check consistency of) shipment and disposal (Example: IC-card developer)



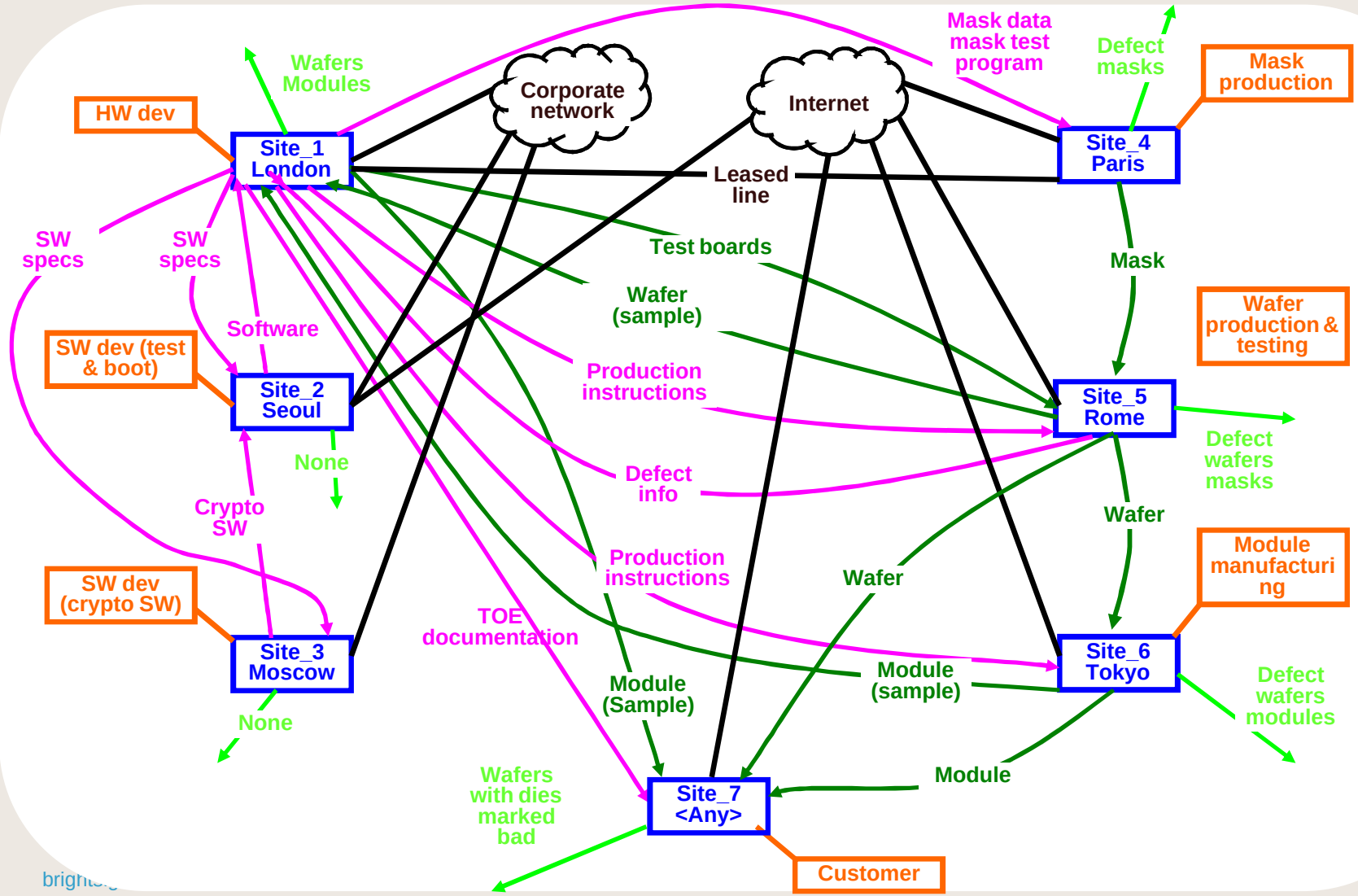
Obtaining and reporting the overview (12)

Step 4f: For site 6 add (and check consistency of) shipment and disposal (Example: IC-card developer)



Obtaining and reporting the overview (13)

Step 5: For site 7 check consistency of shipment and disposal (Example: IC-card developer)



Obtaining and reporting the overview (14)

Comments about the overview picture shown before

- Step 1,2 and 3: Which sites are involved, what do they do and how are they interconnected using networks
  - Possible ways of determining this:
    - Read the ALC documentation
    - Talk with the developer trying to make the list of sites.

    Remark: Though this step seems simple it regularly happens that during a site audit an additional site pops up.
  - To check correctness / completeness it is essential for the evaluator to:
    - Know the different components of the TOE
    - Understand the development and manufacturing steps

Obtaining and reporting the overview (15)

Comments about the overview picture shown before

- Step 4a: For site 1 add shipment and disposal
  - For logical shipment the picture has to be used to check whether shipment is consistent with the IT networks.
  - Physical shipment and disposal have to be consistent
  - Disposal of broken or obsolete data carriers (e.g. harddisks, CDs etc) is not included in the picture as this typically happens in all sites.

Obtaining and reporting the overview (16)

Comments about the overview picture shown before

- Step 4b through 4f: For site 2 through 6 add shipment and disposal
  - For logical shipment the picture has to be used to check whether shipment is consistent with the IT networks.
  - Physical shipment and disposal have to be consistent
  - Disposal of broken or obsolete data carriers (e.g. harddisks, CDs etc) is not included in the picture as this typically happens in all sites.
  - Consistency of already drawn shipments in the picture has to be checked.

Obtaining and reporting the overview (17)

Comments about the overview picture shown before

- Step 5: For site 7 (customer) check consistency of shipment and disposal
  - This step is the result of combining ALC and AGD: For CC 3.1 sending of the TOE is assessed in ALC_DEL while reception is assessed in AGD_PRE.

Remark: The CEM does not ask the evaluator to explicitly check for consistency between shipping procedure (ALC_DEL) and receiving (AGD_PRE).

Obtaining and reporting the overview (18)

About the overview picture shown before in general

- The overview picture is turns out to be very useful:
  - While performing a site audit (to check consistency and completeness)
  - While performing the CEM ALC work units (to check consistency and completeness)
  - To include in the report (to provide an overview to the scheme)
  - To recall the situation after some time of other activities (to refresh my memory)

- Making such picture
  - Does not happen in one day.
  - Involves reading the ALC documentation.
  - Talking to the developer helps.
  - Could the developer produce the picture?
    - Maybe, if not too many parties are involved.

    Remark: I am convinced making this picture would help the developer too. Maybe this presentation will help having the developer realize the value of this picture.

Determining whether the security measures are sufficient

Who/what determines what measures are required?

- For CC 3.1 the CEM (e.g. ALC_DVS.2-2) now explicitly relates this to the vulnerability analysis (AVA).
- The Security Target / Protection profile might include additional requirements.
- There might be additional CC requirements (such as the upcoming Joint Interpretation Library – Site visits guidance) that is applicable to IC-cards).
- There might be additional scheme specific requirements

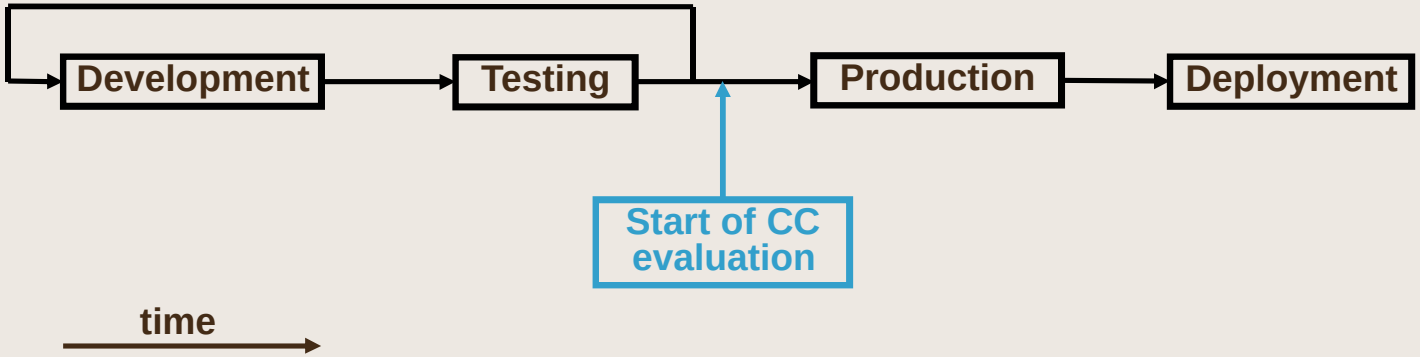
In addition:

The required measures vary based upon the TOE and its state.

Conclusion: Not always easy to determine. (For IC-cards I hope JIL will help)

An inherent weakness of ALC for new evaluations

Timeline for product development up until deployment:



What if there was an issue with site security during development or testing?

Re-use of evidence for ALC by the developer

- The CC does not allow to build upon non-CC certificates
- The evidence for ISO 9000/9001 or similar is very usable for ALC.
- A site having a ISO 9000/9001 certificate has documented procedures which by itself helps enormously in passing a CC certification
- Missing: these ISO9000/9001 standards do not incorporate security

Questions?

Contact information

Note: the name “TNO ITSEF”
has changed to “Brightsight”

Brightsight BV
Delftechpark 1
2628 XJ Delft
The Netherlands

Telephone: +31-15-269 2500
FAX: +31-15-269 2555
Email: info@brightsight.com
Web: http://www.brightsight.com/