# Security Assurance Profile
# for Large and heterogeneous telecom and IT infrastructures

Bertrand Marquet, Samuel Dubus
Alcatel-Lucent Bell Labs France
91620 Nozay, France

Christophe Blad
Oppida,
78180 Montigny-le-Bretonneux, France

## 1. Introduction

*The EU-Eureka-Celtic project BUGYO has investigated how the assurance for services which run on large and complex infrastructures can be modelled [1], measured and monitored continuously [3] based on a six-step methodology relaying on a taxonomy of 5 discreet levels of security assurance [2]. But, the methodology remains highly dependent on expertise to determine risk exposures, express assurance needs and consequently measurement requirements for a given targeted infrastructure, the target of measurement.*

*To reduce this dependence on expertise and propose a common and recognized view, the second phase of the BUGYO Project, the BUGYO Beyond project has introduced the concept of assurance profile as a guideline and best practice to deploy a security assurance measurement infrastructure.*

*We present in this extended abstract, the concept of Security Assurance profile as a tool to express requirement of security assurance of large and heterogeneous infrastructures to gain confidence in services running on those infrastructures thus reducing proactively risk exposure of those infrastructures.*

*The approach is similar to ISO15408 (Common Criteria) protection profile [4] which determine for a type of product security and assurance requirements as a help to determine security target for security certifications.*

**Keywords:** Infrastructure, Measurement, Model, Profile, Security Assurance.

## 2. Assurance Profile

### Target of Measurement

An Assurance Profile (AP) refers to a particular service infrastructure. It defines a Target of Measurement (TOM) as the minimal part of this infrastructure that needs to be measured continuously in order to reach a certain level of security assurance for a service globally. The Assurance Profile introduces the concept of Security Assurance View (SAV). Each Security Assurance View, defined in an Assurance Profile, gives a particular representation of the security assurance of the Target of Measurement. An Assurance Profile contains one or several Security Assurance Views.

Each Security Assurance View has a specific focus (e.g. a regulation, a standard, a security policy or list of requirements etc.). Examples of Security Assurance Views are (but not limited to):

- A functional security assurance view,
- A security policies assurance view,
- A regulation security assurance view,
- A standard security assurance view,
- A geographical security assurance view,
- A set of equipment security assurance view,
- An application security assurance view.

During deployment of the service infrastructure these views will contribute, be instantiated combined or refined to build a model for the Target of Measurement.

Figure 1 depicts concepts of Target of Measurement and Security Assurance views.

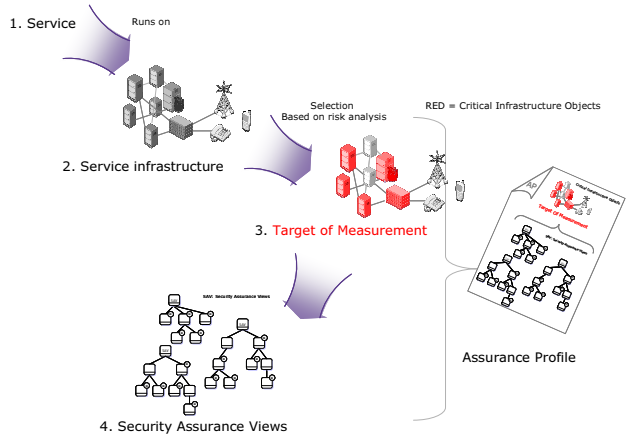


Figure 1 from Service to Assurance Profile

An Assurance Profile is typically a statement of operational assurance measurement needs implemented by a defined and common set of operational assurance metrics. The use may differ between different actors.

An Assurance Profile is a statement of needs in which equipment vendors, solution providers, service integrators and operators define a common set of security assurance metrics on an agreed Target of Measurement. An AP gives a means of

referring to this set, and facilitates futures evaluation against these needs.

An Assurance Profile can be considered as a specific angle of view for measuring the security assurance of a service infrastructure. Then, an entity (e.g. an operator or a corporate) may choose to implement different monitoring views of the security assurance of a service infrastructure, which may relate to several different Assurance Profiles.

An Assurance Profile could therefore typically used as:

- Part of requirement specification for a specific consumer or group of consumers, who will only consider buying a specific type of service if it meets the Assurance Profile.
- Part of a regulation from a specific regulatory entity, who will only allow a specific type of Service to be used if it meets the Assurance Profile.
- A baseline defined by a group of service providers, who then agree that all services that they provide of this type will conform to the agreed AP.

Though, this does not preclude other uses.

## 3. Assurance profile structure and content

The following diagram illustrates how an Assurance Profile is articulated and how to build it. It shows as well dependency and operations to gather information.

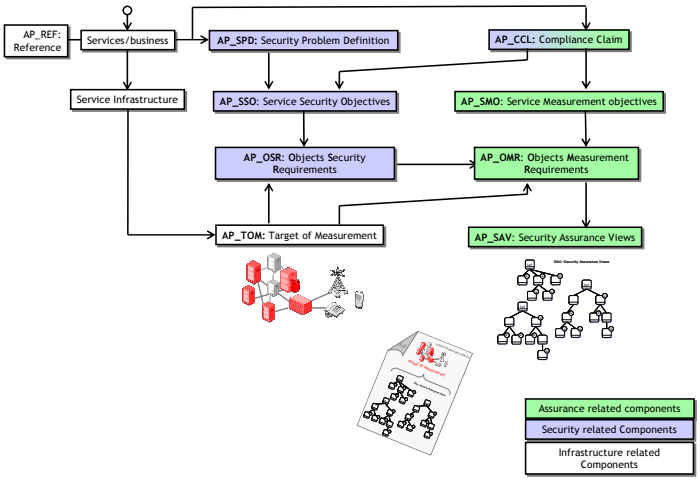


Figure 2 Assurance Profile Structure

The structure of an Assurance Profile is composed of three (3) types of components: infrastructure related components, security related components and assurance related components. An Assurance Profile represents a common and coherent understanding on how security and assurance should be addressed for a Target of Measurement as described in infrastructure related components.

The structure of an Assurance Profile is top down, from the service to a target of measurement associated with a set of security assurance views. The entry point of the Assurance Profile is a telecommunication service or a specific business associated with this telecommunication service - e.g. IP-VPN service of a large company or the specific business associated with the VoIP service in the triple-play offer of a Carrier. This service is running on an infrastructure. In order to reduce the complexity, an Assurance Profile and more generally the security assurance measurement scope will focus only on critical components of this infrastructure on which security safeguards are deployed. The set of critical infrastructure objects that will be measured, defines the Target of Measurement as defined previously. All these components are called *infrastructure Objects*.

Concerning *security related components*, the Assurance Profile is providing a presentation of the security problem that the service is facing and the security requirements that should be deployed to address those problems. This is addressed in the "Security Problem Definition" component. This component is refined into Services Security Objectives. Those Services Security Objectives may also be derived from the claimed compliance to standards or regulations. Those Service Security Objectives are then refined into Objects Security Requirements.

Concerning *assurance related components*, the Assurance Profile is providing first a compliance claims which describe which standards, regulations, or any specific document that is relevant to the security of the service. Those compliance claims are derived into Services Measurement Objectives which are then derived into Objects Measurement Requirements. Those requirements also depend on Objects Security Requirements.

Having defined measurement objectives, they are selected and combine to constitute different security assurance view related to the concerned service. All these security assurance views will fully describe what need to be deployed and measures on the TOM to obtain service security assurance.

## 4. Implementing security assurance program using an Assurance Profile

The general use of an Assurance Profile is to help the establishing of a continuous assurance measurement program and deploy an associated measurement infrastructure.

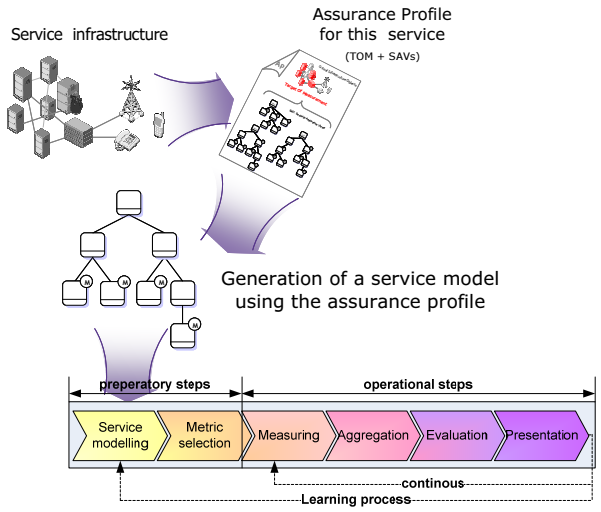


Figure 3 Using an Assurance Profile

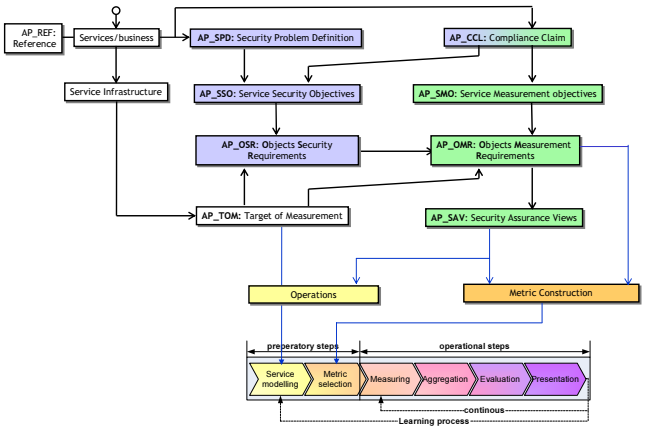


Figure 4 Using Assurance Profile for Assurance model

As depicted in the previous figure, when an operator, a service integrator or a group of users or consumers want to establish such a program, they should first look if there is an existing Assurance Profile corresponding to their service. Then, different cases could happen, as shown in figure 5. Each of the cases is associated with one or several operations.

Operations on protection profiles are linked to how they will be used to generate the service model.

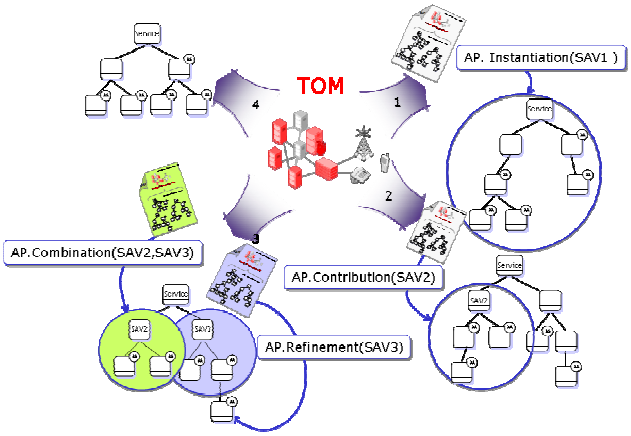


Figure 5 Operations on Assurance Profile views

The first case is the simplest one. In this case, an Assurance Profile exists for the concerned service and one of the Security Assurance View of this profile matches the specific case to be addressed. In this case, the person in charge of establishing the model for its specific TOM has just to instantiate the appropriate view. This operation is called instantiation and concerned one view of the Assurance Profile.

In the second case, one assurance view is selected to generate a part of the model. The remaining infrastructure objects and metrics will be expressed specifically for the model without using the Assurance Profile. The operation is called selection as the model is partially based on one assurance view of the model.

The third case is using an Assurance Profile to generate the model by combining several view of the model as well as refining one or several combined view. The combination operation consists in adding two security assurance views to create a new one at the upper level.

The fourth case represents the worst case as no Assurance Profile exists for the service. The model has to be entirely built by the expert.

## 5. Conclusion

We introduced here the assurance profile concept. This concept is important in risk management as it allows identifying precisely what need to be measured to have confidence that security deployed is conformed to what have been specified in order to reduce risk exposure and potential damage.

## 6. References

*[1] Albin Zuccato, Bertrand Marquet, Serge Papillon, Magnus Alden - Service oriented modelling of communication infrastructure for assurance - in the proceedings of the IEEE workshop on Information Assurance, 2006.*

*[2] Albin Zuccato, Samuel Dubus, Evren Bulut - Methodology for service-oriented management of security assurance in communication infrastructures - in proceedings of the 11th IEEE High Assurance Systems Engineering Symposium, 2008.*

*[3] Evren Bulut, Djamel Khadraoui, Bertrand Marquet - Multi-agent based security assurance monitoring system for telecommunication infrastructure – in The Fourth IASTED International Conference on Communication, Network and Information Security, CNIS 2007.*

*[4] Common criteria, ISO15408 Part 1.*
***www.commoncriteriaportal.org***