

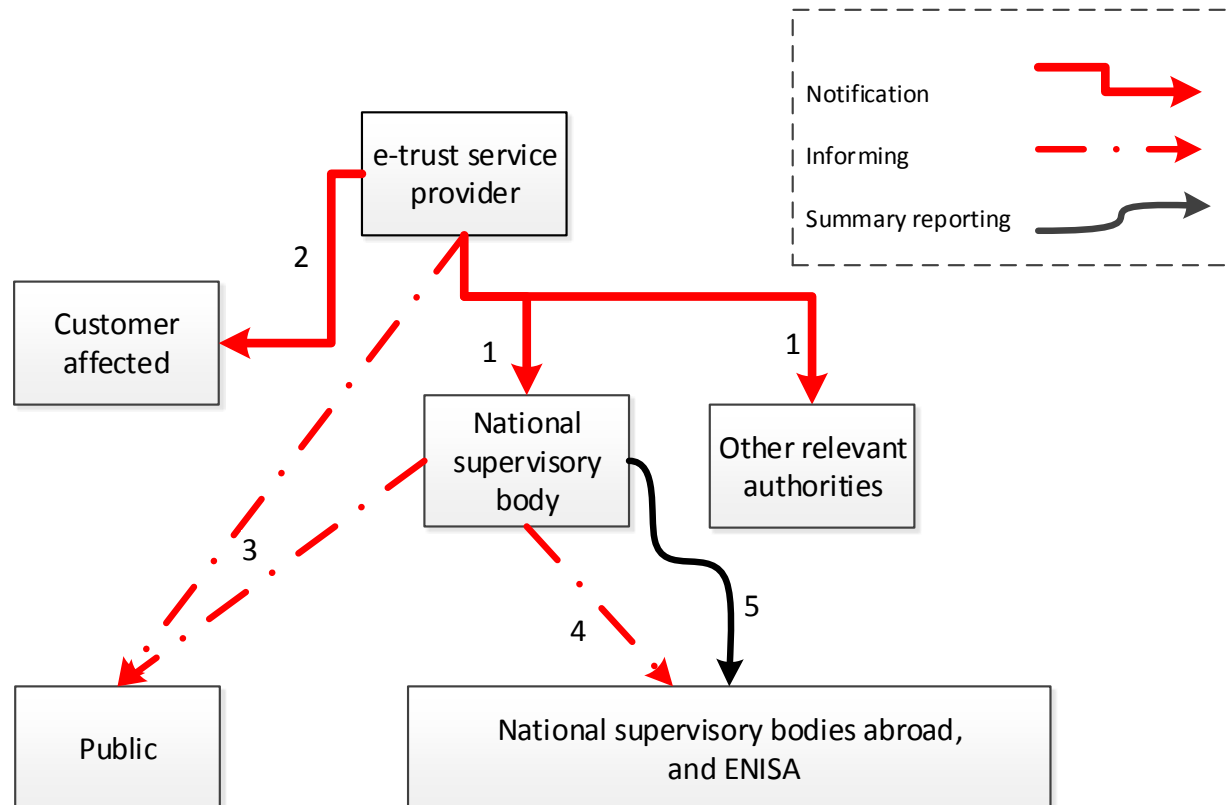


The role of ENISA and incident reporting under article 19 eIDAS regulation

Konstantinos Moulinos | ENISA Trust Services Forum 2015 | Brussels | 30th of June



Overview of reporting flows in Article 19



ENISA in article 19 of eIDAS

ENISA runs an expert group: Scope of this group

- Scope and terms of reference of ENISA Article 19 group
- Scope is Article 19 – eTrust services providers
- Group is run by ENISA, ENISA will liaise with relevant industry groups
- EC supports this group and will liaise with other/existing groups or legislation (such as NIS directive).
- Main topic is security breach reporting (par 19.2)
- Simple, streamlined, harmonized, fitting existing national structures/authorities
- Security practices (par 19.1) are relevant but this group will not establish standards or new practices but liaise with existing standards and ongoing work

Goal is to develop non-binding technical guidelines for supervisory bodies on article 19 (to support their work).

Working with experts from these bodies

FESA is part of the consultation

The role of ENISA



The role of ENISA and incident reporting under article 19 eIDAS
regulation | Konstantinos Moulinos

Article 19 incident reporting guidelines

First consultation with authorities ended

The new version is ready for comments by TSPs and FESA

The final document is expected by end of October 2015

This guide will contain

- List common threats, vulnerabilities, attack scenarios
- Thresholds for notifying
- A notification template for TSPs
- An annual summary reporting template
- Thresholds for annual summary reporting
- A template for questions to ask the reporter (secondary report, causes)

Roadmap

Summer 2015

- 2nd draft of the incident reporting framework (with TSPs and FESA)
- draft report on use cases (by ENISA)

September 2015

- 3rd draft of incident reporting framework (if needed)
- consultation on use cases and functional specs (with the expert group)

October 2015

- 4th meeting
- Incident reporting framework final draft (ENISA)
- final draft of use cases – functional specs (ENISA)

End of 2015 – functional specification for extending online incident reporting tool (OIRT)

Spring 2016

- pilot OIRT with supervisory bodies
- use the input from the pilot to finalize incident reporting framework (before summer 2016)

Autumn 2016 – Deepen the level of technical detail in the security measures work. Address the issue of supervising the (unlisted) non-qualified TSPs

1/1/2017: Authorities are capable of submitting their national reports using the OIRT



Thank you



PO Box 1309, 710 01 Heraklion, Greece



Tel: +30 28 14 40 9710



info@enisa.europa.eu



www.enisa.europa.eu

