# Service Criticality Form

RPKI

## Introduction

This form is used to gather input from the community on service criticality. The framework is detailed in a RIPE Labs article: https://labs.ripe.net/author/razvano/service-criticality-framework/

Service criticality has three main components:

***Confidentiality****: What is the highest possible impact of a data confidentiality-related incident (data leak)?*

***Integrity****: What is the highest possible impact of a data integrity-related incident (hacking)?*

***Availability****: What is the highest possible impact of a service availability-related incident (outage)? All of our services are designed with at least 99% availability, so please consider outages of up to 22 hours per quarter.*

## Service Overview

| | |
|---|---|
| Service purpose | The RIPE NCC RPKI Service is theTrust Anchor (TA) for Eruope, the Middle East and Central Asia. It is comprised of::<br>* RPKI Dashboard (in the LIR portal)<br>* Repositories (rsync/RRDP)<br>* Certification Authorities (CAs)<br>* RPKI Management API<br>* Hardware Security Modules (HSMs)<br>* Datasets |
| Service owner(s) | Nathalie Trenaman |
| Stakeholders | Internally: Registration Services, Legal, Information Security and Compliance, Community and Engagement, Learning and Development, Information Technology, Software Engineering, Research and Development<br><br>Externally: Mainly the RIPE Routing Working Group |
| Types of data the service stores or processes | Internet number resources (IP addresses and AS Numbers)<br>User authentication (SSO)<br>RPKI related objects such as: Certificates, Manifests, CRLs, ROAs.<br>Public keys<br>User Private keys (for Hosted RPKI) |
| Critical service areas | RPKI Core infrastructure |

| | |
|---|---|
| | Hardware Security Modules<br>RRDP Repositories<br>rsync Repositories |
| Non-critical service areas | LIR Portal<br>REST API |

# Impact areas

## Global Routing

| **Global Routing** | **Low** | **Medium** | **High** | **Very High** |
|---|---|---|---|---|
| | No/negligible impact | Limited reachability issues | Widespread reachability issues | Widespread and persistent reachability issues |

| **Incident Impact on Global Routing** | **Incident Severity** |
|---|---|
| ***Confidentiality: (Impact level of incidents such as data leaks)*** | |
| All information in RPKI (except for private keys) is publicly available.<br>All keys are stored in an HSM, therefore we estimate the risk as medium. | **Medium** |
| ***Integrity: (Impact level of incidents such as hack attempts)*** | |
| Trust in the integrity of RPKI is essential.<br>If someone has unauthorised access to the LIR Portal, they could delete a CA or change ROAs which could have an impact on global routing. Also, an unauthorised transfer of resources or a breach would impact the integrity of the repository. | **Very High** |
| ***Availability: (Impact level of service outage incidents, up to 22 hours per quarter)*** | |
| An outage would cause an inability to create, modify and delete ROAs or other RPKI signed objects, and create or delete CAs and repositories.<br>If a repository is down, Relying Party software will rely on their cache until objects expire.<br>In case RRDP repositories experience an outage, Relying Party software should fall back to rsync. Our RPKI infrastructure and HSMs are redundant.<br>Should an outage last so long that objects expire, this would cause operational and reputational damage, security would go down, and exploitation may occur. | **Very High** |

## IP addresses and AS Numbers

| **IP addresses and AS Numbers** | **Low** | **Medium** | **High** | **Very High** |
|---|---|---|---|---|
| | No/negligible impact | Local disruptions (registration information not being available for some entities) | Regional disruptions (registration information not being available for the RIPE NCC region) | Global disruptions (lack of registration information for all AS Numbers and IP addresses) |

| **Incident Impact on IP Addresses and AS Numbers** | **Incident Severity** |
|---|---|
| ***Confidentiality: (Impact level of incidents such as data leaks)*** | |
| No impact in this area | **Low** |
| ***Integrity: (Impact level of incidents such as hack attempts)*** | |
| No impact in this area | **Low** |
| ***Availability: (Impact level of service outage incidents, up to 22 hours per quarter)*** | |
| No impact in this area | **Low** |

## Global DNS

| **Global DNS** | **Low** | **Medium** | **High** | **Very High** |
|---|---|---|---|---|
| | No/negligible impact | Local DNS issues | Widespread DNS issues | Widespread and persistent DNS issues |

| **Incident Impact on Global DNS** | **Incident Severity** |
|---|---|
| ***Confidentiality: (Impact level of incidents such as data leaks)*** | |
| No impact in this area | **Low** |
| ***Integrity: (Impact level of incidents such as hack attempts)*** | |
| No impact in this are | **Low** |
| ***Availability: (Impact level of service outage incidents, up to 22 hours per quarter)*** | |
| No impact in this area | **Low** |