




# CERT MBANK

---

RFC 2350

|                   |   |
|-------------------|---|
| <b>CERT mBank</b> |  |
| RFC 2350 v.1.0    |   |

## Document Control

### Approval


|              | <b>Name</b>      | <b>Date</b> |
|--------------|------------------|-------------|
| Prepared by: | Jaroslav Stasiak | 2017.10.20  |
| Approved by: | Jaroslav Gorski  | 2017.10.26  |

### History

| <b>Date</b> | <b>Revision</b> | <b>Author</b>    | <b>Modification</b> |
|-------------|-----------------|------------------|---------------------|
| 2017.10.20  | 1.0             | Jaroslav Stasiak | Initial version     |
|             |                 |                  |                     |

## Summary:

|   |   |
|---|---|
| Document Control .....  | 2 |
| 1. Document information .....                                     | 4 |
| 1.1. Date of last update.....                                     | 4 |
| 1.2. Distribution list for notifications.....                     | 4 |
| 1.3. Location where this document may be found .....              | 4 |
| 1.4. Authenticating this document .....                           | 4 |
| 2. Contact Information.....                                       | 4 |
| 2.1. Name of the Team.....  | 4 |
| 2.2. Address .....  | 4 |
| 2.3. Date of Establishment.....                                   | 4 |
| 2.4. Time Zone.....   | 4 |
| 2.5. Telephone Number .....                                       | 4 |
| 2.6. Facsimile Number.....  | 5 |
| 2.7. Other Telecommunication.....                                 | 5 |
| 2.8. Electronic Email Address .....                               | 5 |
| 2.9. Public Keys and other Encryption Information .....           | 5 |
| 2.10. Team Members .....  | 5 |
| 2.11. Points of Customer Contact .....                            | 5 |
| 3. Character .....  | 5 |
| 3.1. Mission Statement.....                                       | 5 |
| 3.2. Constituency.....  | 6 |
| 3.3. Sponsorship / affiliation .....                              | 6 |
| 3.4. Authority.....   | 6 |
| 4. Policies.....  | 6 |
| 4.1. Types of Incidents and Level of Support.....                 | 6 |
| 4.2. Co-operation, Interaction and Disclosure of Information..... | 6 |
| 4.3. Communication and Authentication.....                        | 7 |
| 5. Services .....   | 7 |
| 5.1. Incident Response .....                                      | 7 |
| 5.2. Proactive Activities .....                                   | 8 |
| 6. Incident reporting Forms .....                                 | 8 |
| 7. Disclaimers.....   | 8 |

|                   |   |
|-------------------|---|
| <b>CERT mBank</b> |  |
| RFC 2350 v.1.0    |   |

## 1. Document information

This document contains the formal description of CERT mBank based on the RFC 2350. It provides information about CERT mBank Team, its communication channels and services.

### 1.1. Date of last update

This is the initial 1.0 version, released on October, 20<sup>th</sup> 2017

### 1.2. Distribution list for notifications

There is no distribution list for notifications.

### 1.3. Location where this document may be found

The current and latest version of this document is available in PDF format on the mBank website. Its URL is:

<https://www.mbank.pl/pdf/inne/cert-mbank-rfc2350.pdf>

### 1.4. Authenticating this document

The text version of this document has been signed with the CERT mBank PGP key. The signature is available on the mBank website. Its URL is:

<https://www.mbank.pl/pomoc/info/certyfikat/cert-mbank.asc>

## 2. Contact Information

### 2.1. Name of the Team

CERT mBank

Full Name: Cyber Security Response Team of mBank S.A.

### 2.2. Address

mBank S.A.  
CERT mBank  
74 Kilinskiego Str.  
90-257 Lodz,  
Poland

### 2.3. Date of Establishment

CERT mBank was established in December 2016


### 2.4. Time Zone

GMT +0100 - Central European Time (CET)

GMT +0200 - Daylight Saving Time (from last Sunday in March to last Sunday in October)

### 2.5. Telephone Number

+48 42 218 67 67

|                   |   |
|-------------------|---|
| <b>CERT mBank</b> |  |
| RFC 2350 v.1.0    |   |

## 2.6. Facsimile Number

+48 42 2186724

## 2.7. Other Telecommunication

None available

## 2.8. Electronic Email Address

All incident reports should be submitted to <cert(at)mbank.pl>

## 2.9. Public Keys and other Encryption Information

mBank CERT PGP Key information:

Key ID: 0x873D6686

Fingerprint: 9E9D11C6D3B85233D3E7FFD1038048FE873D6686

The public key and its signature can be found at the usual large public key servers, or on CERT mBank information page:

<https://www.mbank.pl/bezpieczenstwo/certyfikaty/>

## 2.10. Team Members

CERT mBank's team leader is Jaroslaw Stasiak. The rest of the team consists of several IT security analyst.

## 2.11. Points of Customer Contact

The preferred method for contacting with CERT mBank is via e-mail. For general inquiries please use address:

<cert(at)mbank.pl>


A duty security analyst can be contacted at this email address during hours of operation (24/7/365). If necessary, urgent cases can be reported directly by phone (+48 42 218 67 67 ) during Polish business hours.

# 3. Character

## 3.1. Mission Statement

The main purposes of CERT mBank are:

- to prevent and anticipate computer security incidents by implementing adequate processes, tools, policies to improve the reactivity in case of an incident,
- to provide 24x7x365 adequate operational support for handling serious computer security incidents which can affect mBank's assets and interests including mBank's Customers, Employees, Partners and Shareholders,
- to assist and support mBank employees in implementing proactive measures to reduce the risks of computer security incidents, in particular by providing a consultancy and education services,

|                   |   |
|-------------------|---|
| <b>CERT mBank</b> |  |
| RFC 2350 v.1.0    |   |

## **3.2. Constituency**

CERT mBank supports incident response and security services for mBank employees and its customers.

## **3.3. Sponsorship / affiliation**

CERT mBank is a private CERT operating in the financial sector. It is owned and fully financed by mBank S.A.

It maintains relationships with different CERTs/CSIRTs in Poland and in Europe as a member of Trusted Introducer since December 2016.

<https://www.trusted-introducer.org/directory/teams/cert-mbank.html>

## **3.4. Authority**

CERT mBank operates under the auspices of, and with authority delegated by, the Chief Security Officer of mBank S.A.

# **4. Policies**

## **4.1. Types of Incidents and Level of Support**

CERT mBank is authorized to address and handle all types of computer security incidents or cyberattacks which occurs at its constituency (see section 3.2).

All the incident reports received by CERT mBank are analysed, classified and prioritized according to internal regulations so that an efficient and appropriate level of service is provided.


Resources will be assigned according to the following priorities:

- threats to the physical safety of human beings,
- root or system-level attacks on any part of the backbone network infrastructure, public service or other core mBank systems,
- compromise of restricted confidential service accounts or software installations, in particular those used for core/critical applications containing confidential data or those used for system administration,
- denial of service attacks or any other attempts of limiting availability of services or information processed in core systems,
- large-scale attacks of any kind, e.g. social engineering aimed at employees or bank customers, malware spread or distribution, information leakage,
- threats, harassment, and other criminal offenses involving individual user accounts,
- compromise of individual user accounts on multi-user systems, compromise of desktop systems,
- forgery and misrepresentation or other security-related violations of local rules and regulations.

Types of incidents other than those mentioned above will be prioritized according to their apparent severity and extent.

## **4.2. Co-operation, Interaction and Disclosure of Information**

CERT mBank will cooperate with other organizations like CERTs/CSIRTs in the field of computer security. This cooperation also includes the exchange of information regarding security incidents and vulnerabilities. Nevertheless, CERT mBank operates under the legal

|                   |   |
|-------------------|---|
| <b>CERT mBank</b> |  |
| RFC 2350 v.1.0    |   |

restrictions imposed by the Polish law, e.g. Personal Data Protection Law or Banking Act about banking secrecy.

Because of the obligation of protecting the privacy of its constituency, CERT mBank (under normal circumstances) pass on available for sharing information in an anonymized way only.

It will only provide information to other parties with the sole purpose of facilitating the tasks of containment, eradication and recovery of incidents under the general principle of providing the minimum information possible.

### **4.3. Communication and Authentication**

CERT mBank protects sensitive information in accordance with relevant Polish and European regulations and policies.

For normal communication not containing sensitive information, CERT mBank might use conventional methods like unencrypted e-mail or telephone. For secure communication PGP-encrypted e-mail will be used. If it is necessary to authenticate a person before communicating, this can be done either through existing webs of trust (e.g. TF-CSIRT, FIRST) or by other methods like call-back, mail-back or even face-to-face meeting if necessary.

CERT mBank also recognizes and supports the ISTLP (Information Sharing Traffic Light Protocol).

## **5. Services**

### **5.1. Incident Response**

CERT mBank will assist system administrators in handling the technical and organizational aspects of incidents. In particular, it will provide assistance or advice with respect to the following aspects of incident management:

#### **5.1.1 Incident Triage**

- determining whether an incident is authentic
- determining the extent of the incident, assessing and prioritizing it

#### **5.1.2 Incident Coordination**


CERT mBank incident coordination includes:

- determining the initial cause of the incident (vulnerability exploited),
- facilitating contact with other sites which may be involved,
- facilitating contact with appropriate security teams and/or appropriate law enforcement officials, if necessary,
- composing announcements to users, if applicable.
- making reports,

#### **5.1.3 Incident Resolution**

CERT mBank incident resolution includes:

- technical assistance and investigation, which may include analysis of compromised systems,
- eradication or elimination of the cause of a security incident (the vulnerability exploited), and its effects,

|                   |   |
|-------------------|---|
| <b>CERT mBank</b> |  |
| RFC 2350 v.1.0    |   |

- collection of evidences, to start legal actions if necessary,
- recommendation of the security improvements to system administrators and business managers (post-mortem).

In addition, CERT mBank will collect statistics concerning incidents which occur within or involve its constituency, and will notify the community as necessary to assist it in protecting against known attacks.

## **5.2. Proactive Activities**

Proactive services provide means to reduce the number of actual incidents by giving proper and suitable information concerning potential incidents to the constituency. CERT mBank will perform proactive activities to improve performance and capabilities such as:

- observation of current trends in technology and security,
- awareness campaigns (e.g. about current threats and attacks),
- trainings and simulation activities,
- cybersecurity support and advices,
- vulnerability scanning,
- forensics and malware analysis,
- intelligence reporting,

## **6. Incident reporting Forms**

Through email or phone call.

## **7. Disclaimers**

While every precaution will be taken in the preparation of information, notifications and alerts, CERT mBank assumes no responsibility for errors or omissions, or for damages resulting from the use of the information it provides