RFC2350 of SAX.CERT

1. Document Information

1.1 Date of Last Update

This is version 1.3 of 3rd January 2018.

1.2. Distribution List for Notifications

E-mail notifications of updates are sent to the Trusted Introducer Service for incident response and security teams https://www.trusted-introducer.org

Please address any questions about updates to sax.cert@cert.sachsen.de

1.3. Locations where this Document May Be Found

The current version of this document is available internally within SID and will be published at http://www.cert.sachsen.de.

2. Contact Information

2.1. Name of the Team

Full name: SAX.CERT

Short name: SAX.CERT

2.2. Address

Postal Address:

Staatsbetrieb Sächsische Informatik Dienste
z.Hd. SAX.CERT-Team
Riesaer Str. 7
01129 Dresden
Germany

2.3. Time Zone

GMT01/GMT02(DST)

2.4. Telephone Number

+49 351 7999 77 99

2.5. Facsimile Number

Cryptofax +49 351 8473 23 96

2.6. Other Telecommunication

Cryptofax +49 351 8473 23 96

2.7. Electronic Mail Address

Please send incident reports related to our constituency to: sax.cert@cert.sachsen.de

2.8. Public Keys and Encryption Information

2.8.1 PGP / GnuPG

The recent PGP key is:

0xA478B1C2 SAX.CERT <sax.cert@cert.sachsen.de>

Fingerprint: 40C3 7E86 5A3E 9C61 5D25 7B1C A814 30A3 A478 B1C2

The key is published at public PGP-keyservers (e.g. keyserver.pgp.com).

2.8.2 S/MIME

The valid X.509 certificate for sax.cert@cert.sachsen.de is:


```
-----BEGIN CERTIFICATE-----
MIIGFDCCBPygAwIBAgIHGZjFqHWZpjANBgkqhkiG9w0BAQsFADCBwDELMAkGA1UE
BhMCREUxEDAOBgNVBAgTB1NhY2hzZW4xEDAOBgNVBAcTB0RyZXNkZW4xGjAYBgNV
BAoTEUZyZWlzdGFhdCBTYWNoc2VuMTIwMAYDVQQLEylTYWVjaHNpc2NoZXMgU3Rh
YXRzbWluaXN0ZXJpdW0gZGVzIElubmVybjEaMBgGA1UEAxMRU2FjaHNlbiBHbG9i
YWwgQ0ExITAfBgkqhkiG9w0BCQEWEnBraUBzbWkuc2FjaHNlbi5kZTAeFw0xNTA2
MTEwODM0MzJaFw0xODA2MTAwODM0MzJaMHwxCzAJBgNVBAYTAkRFMRowGAYDVQQK
DBFGcmVpc3RhYXQgU2FjaHNlbjE1MDMGA1UECwwsU3RhYXRzYmV0cmllYiBTYWVj
aHNpc2NoZSBJbmZvcm1hdGlrIERpZW5zdGUxGjAYBgNVBAMMEUdSUDogQ0VSVCBT
YWNoc2VuMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAqOhde6CKTGgh
bEXjpEPaUfzgRl2TxZs0F37LJ6ia+NJOAzLJFDh/k/CU313Bx9bZRff8YgoWXcok
/jZOi87DytKAn/nWPnrfWMd+UF46hLs1yN7gfiOKfl2PsEAEJZkkm6MDJiVodsoN
ZoGzyunF8mKRP7ZtIkcqEy+BG3jwzYLIQe9mueBsTg4Q/o3TjgQXItXfa7kxtNZq
HPExp+DlUxSLboD6pCRyoqgsw3MOOmCcO/XjZSHLjC4dMs8vLLFJUsewU/jeYxDk
khn0QZ83buQPZJ5jcVn3GsAuiSLItZeoZ32iInMLOwgzaRoHidQgXXtanEx/GUtr
pKTehPtk1wIDAQABo4ICVDCCAlAwQAYDVR0gBDkwNzARBg8rBgEEAYGtIYIsAQEE
AwMwEQYPKwYBBAGBrSGCLAIBBAMBMA8GDSsGAQQBga0hgiwBAQQwCQYDVR0TBAIw
ADALBgNVHQ8EBAMCBeAwHQYDVR0lBBYwFAYIKwYBBQUHAwIGCCsGAQUFBwMEMB0G
A1UdDgQWBBStrw0KybehwVFA7VKefLxBIKZtdjAfBgNVHSMEGDAWgBTNzv6x//ku
5Jap/yvjLYAdjkqY9TAjBgNVHREEHDAagRhzYXguY2VydEBjZXJ0LnNhY2hzZW4u
ZGUwgY8GA1UdHwSBhzCBhDBAoD6gPIY6aHR0cDovL2NkcDEucGNhLmRmbi5kZS9z
```

YWNoc2VuLWdsb2JhbC1jYS9wdWIvY3JsL2NhY3JsLmNybDBAoD6gPIY6aHR0cDov
L2NkcDIucGNhLmRmbi5kZS9zYWNoc2VuLWdsb2JhbC1jYS9wdWIvY3JsL2NhY3Js
LmNybDCB3QYIKwYBBQUHAQEEgdAwgc0wMwYIKwYBBQUHMAGGJ2h0dHA6Ly9vY3Nw
LnBjYS5kZm4uZGUvT0NTUC1TZXJ2ZXIvT0NTUDBKBggrBgEFBQcwAoY+aHR0cDov
L2NkcDEucGNhLmRmbi5kZS9zYWNoc2VuLWdsb2JhbC1jYS9wdWIvY2FjZXJ0L2Nh
Y2VydC5jcnQwSgYIKwYBBQUHMAKGPmh0dHA6Ly9jZHAyLnBjYS5kZm4uZGUvc2Fj
aHNlbi1nbG9iYWwtY2EvcHViL2NhY2VydC9jYWNlcnQuY3J0MA0GCSqGSIb3DQEB
CwUAA4IBAQAIUEgqZd9h38GHDA63K9YsTRpsyiXGiA8k69vGNJu3VvVxzH0NpeTv
iOeWl9XLyV+frCjp3zCnbjcrKmLBFdAyXFrfwu20dkEMysDP6GeNXBs+n+ZDvD3m
8S6icXONzPp/9zZ3NpJrr5w/PmaoyR71+YIgiXmc+XllQCE/4KCbI780Jm6ayKXY
YwEBoI/KKdGYBpTnvvcv/UTO/9xBQGtUuaQjocKEiPicYpSRRZH1/f6lSeWpD1jf
G3RCDNI0HnZUs2RiWXSYriSC2s7FpldeNnXqnxTBzUtbz/Gb5Iypm+RcvZFc17wd
DRdajHnWfWMlcjl/kKtcxSdocGiVbCzW
-----END CERTIFICATE-----

You can download the full certification path at <link>.

2.9. Team Members

The team leader:

Christoph Damm <christoph.damm@sid.sachsen.de>
Telephone: +49 351 3264 6630

The list of team members is not public.

2.10. Other Information

N/A

2.11. Points of Customer Contact

The preferred method for contacting SAX.CERT is via e-mail:

For abuse complains please use: sax.cert@cert.sachsen.de

For security incidents use: sax.cert@cert.sachsen.de

Please use secured e-mail if you would like to send us sensitive information.

The mailbox is monitored during regular office hours: Monday to Friday. 08.30-16.30. Except during public holidays in Germany.

3. Charter

3.1. Mission Statement

SAX.CERT is the incident response team for all government institutions and agencies of the Free State of Saxony (Freistaat Sachsen), Germany, and its subsidiaries.

Our mission is to co-ordinate the management and response to security incidents within our constituency.

3.2. Constituency

SAX.CERTs services are available to government authorities of Free State of Saxony, Germany.

3.3. Affiliation

SAX.CERT is run by Staatsbetrieb Sächsische Informatik Dienste.

3.4. Authority

SAX.CERT operates under the auspices of, and with authority delegated by the Saxon State Ministry of Interior.

4. Policies

4.1. Types of Incidents and Level of Support

SAX.CERT is authorized to address all types of security incidents which occur, or threaten to occur, in our Constituency (see 3.2).

Please note that direct support will be only provided to persons employed within government institutions and agencies of the Free State of Saxony, Germany, and its subsidiaries.

We do however read and evaluate all information sent to us regarding potential security events or incidents.

4.2. Co-operation, Interaction and Disclosure of Information

All information communicated to us will be handled with great care regardless of its priority. Confidentiality will be determined according to established practices and standards.

In order to help us in our response, please describe any restrictions of using or sharing the information you have sent us.

SAX.CERT supports the Information Sharing Traffic Light Protocol (ISTLP – see https://www.trusted-introducer.org/ISTLPv11.pdf). Information that is received with an attached ISTLP tag WHITE, GREEN, AMBER or RED will be handled accordingly.

4.3. Communication and Authentication

Please use secured e-mail to communicate sensitive information, especially if ISTLP tags AMBER or RED are used.

5. Services

5.1. Incident Response (Triage, Coordination and Resolution)

SAX.CERT is responsible for the coordination of security incidents in its constituency. It ensures that the information is passed to the person is able to resolve reported issues.

5.1.1 Incident Triage

Incident triage is handled by SAX.CERT

5.1.2 Incident Coordination

Incident coordination is handled by SAX.CERT

5.1.3 Incident Resolution

Incident resolution is handled by SAX.CERT in cooperation with the involved constituents.

5.2. Proactive Activities

SAX.CERT performs the following activities for its constituency:

- Security monitoring
- Awareness building and information sharing within its constituency
- Trend and threat analysis for its constituency

6. Incident reporting Forms

SAX.CERT provides its public web page at http://www.cert.sachsen.de.

Currently, no incident reporting form is available to the public. Instead please use encrypted e-mail. Please make sure to always include your own contact information as well your PGP key if you'd like to receive feedback encrypted as well.

Please provide as much information as possible, when reporting incidents.

For example:

- Type of incident (Spam, Malicious code targeting our constituency, scanning etc.)
- Time and date of all events reported. Please include the time zone the events were reported or detected. This will help us to correlate your information with other events or security incidents.

If you'd like to provide malicious code, please contact us by phone or e-mail. We agree a transfer mechanism avoiding problems with anti-virus tools and intrusion detection systems.

7. Disclaimers

None.