Specification of Kvaser Remote Device Configuration XML Format

Printed Sunday 16th September, 2018

(This page is intentionally left blank.)

Contents

1 About this Manual

This report describes the XML version 4.3 used to create settings for Kvaser BlackBird. It is applicable to the devices listed in Table 1.

Device	Product Number	Product Family
Kvaser BlackBird SemiPro HS	73-30130-00441-2	blackbird
Kvaser BlackBird SemiPro 3xHS	73-30130-00446-7	blackbird
Kvaser BlackBird SemiPro HS/HS	73-30130-00453-5	blackbird
Kvaser BlackBird SemiPro HS OBDII	73-30130-00629-4	blackbird
Kvaser BlackBird v2	73-30130-00671-3	blackbird
Kvaser BlackBird v2 OBDII	73-30130-00675-1	blackbird
Kvaser BlackBird Pro HS v2	73-30130-00983-7	blackbird
Kvaser Ethercan Light HS	73-30130-00713-0	ethercan
Kvaser Ethercan HS	73-30130-00976-9	ethercan
Kvaser DIN-Rail SE400S-X10	73-30130-01059-8	ethercan

Table 1: Kvaser devices and their Product numbers

Throughout this document, we use the name Kvaser BlackBird to mean any one of the different Kvaser BlackBird products listed, unless otherwise noted.

2 XML Settings

This chapter describes all elements used for the settings in Kvaser BlackBird. The structure of this chapter follows the XML file and is divided into areas such as network and security settings.

The XML file must begin with the element KVASER which contains the elements VERSION, PRODUCTFAMILY, DEVICE_ACCESS, CONFIG_PROTECTION, NETWORK, NETWORK_SECURITY, TRAFFIC_ENCRYPTION, WEBSERVER, and REGION_SETTINGS. All elements except NETWORK_SECURITY and TRAFFIC_ENCRYPTION are mandatory.

Please note that some characters are reserved in XML for internal use. These characters must be replaced with entity references when they are used in data; see Table 2.

Name	Value	Character	Description
quot	"	"	double quotation mark
amp	&	&	ampersand
apos	'	’	apostrophe
lt	<	<	less-than sign
gt	>	>	greatert-than sign

Table 2: Reserved characters in XML

It is also possible to use entity references to write e.g. Swedish characters, but it is not needed if the header includes support for ISO-8859-1.

Attributes with value *xml string* must be writable 8-bit ISO 8859-1 characters. The valid characters are number 0x20-0x7E and 0x80-0xFF. Note that the TAB character is not allowed. The xml string must contain at least 1 and at most 31 characters unless the description states otherwise.

2.1 XML File Header

The file must begin with a standard XML file header:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
```

2.2 Format Version (VERSION)

The element `VERSION` is used by the conversion library. The contents of this element is written X.Y and shall be set to 4.3 for the current XML format, specified in this document.

Future versions of this specification will increase the minor version number (Y) if forward compatible changes are made. "Forward compatible changes" means that elements might be added to the specification, but no elements are removed, nor is their meaning changed.

If incompatible changes are made, the major version number (X) will increase. Incompatible changes means that elements are removed from the file, or that the meaning of already defined elements change, or that elements are added and these elements must be processed by all software.

This means that software written to comply with specification version A.B will understand an XML file written to comply with version X.Y, if the following conditions are met.

- A must be equal to X.
- If B > Y, then the software must not require information present in A.B but not in X.Y. Instead it must supply suitable default values if necessary.
- If B < Y, then the software must not report errors when information present in X.Y but not A.B is encountered. Such information must be silently ignored.

Element name: `VERSION`
Children: `None`

```
<VERSION>4.3</VERSION>
```

2.3 Product Family (PRODUCTFAMILY)

The element `PRODUCTFAMILY` is used by the conversion library. It must be set to `Blackbird` for the current XML format.

Note that this value is case insensitive and that whitespace is insignificant. It is recommended that no whitespace is used when writing this element to the XML file.

Element name: `PRODUCTFAMILY`
Children: `None`

```
<PRODUCTFAMILY>Blackbird</PRODUCTFAMILY>
```

2.4 Device Access (DEVICE_ACCESS)

This element sets the visibility of the device on the network.

Element name: `DEVICE_ACCESS`
Children: `None`

```
<!-- Available for all users -->
<DEVICE_ACCESS
  level="PUBLIC"
  password=""
/>
```

Attribute name	Value	Description
level	PUBLIC	Anyone can see and connect to a free device.
	PROTECTED	Anyone can see the device, but a password is required to connect to an avaiable device.
	PRIVATE	Password is required to detect and connect to an existing device.
password	xml string	Can be empty for level PUBLIC. Maximum password length is 31 characters.

Table 3: Attributes for element DEVICE_ACCESS

2.5 Configuration Protection (CONFIG_PROTECTION)

The configuration in the device can be protected with a password. This will require the user to enter a password before accessing the downloaded configuration.

Element name: `CONFIG_PROTECTION`
Children: `None`

```
<!-- Configuration is protected -->
<CONFIG_PROTECTION
  protected="YES"
  password="qwerty12"
/>
```

Attribute name	Value	Description
protected	YES / NO	Select YES if a password is needed to access the configuration in the device.
password	xml string	Can be empty when unprotected. Maximum password length is 31 characters.

Table 4: Attributes for element CONFIG_PROTECTION

2.6 Network (NETWORK)

This element defines network settings for the device.

Element name: `NETWORK`
Children: `None`

```
<!-- Network settings for infrastructure with static ip address-->
<NETWORK
  ssid="MyNetwork"
  operation_mode="INFRASTRUCTURE"
  search_all_channels="YES"
  device_name="BlackBird#42"
  address_type="STATIC"
  device_ip_addr="192.168.171.10"
  device_netmask="255.255.255.0"
  device_gateway="192.168.171.1"
/>
```

Attribute name	Value	Description
device_name	xml string	User defined name in the network. Maximum device name length is 32 characters.
host_name	ASCII string	User defined host name of length 1–31 characters. Valid characters are 'a'-'z', '0'-'9', and '-'. (Optional[1])
address_type	DHCP	Use address type DHCP to rely on a DHCP server to hand out an address to the device.
	STATIC	Use STATIC to select an address manually.
device_ip_addr	decimal dot format	IPv4 address for static address type, written in decimal dot format, e.g. 192.168.171.10 Not required when using DHCP.
device_netmask	decimal dot format	IPv4 netmask for static address type, written in decimal dot format, e.g. 255.255.255.0 Not required when using DHCP.
device_gateway	decimal dot format	IPv4 gateway for static address type, written in decimal dot format, e.g. 192.168.171.1 Not required when using DHCP.

(continued on next page)

[1] If omitted, kvrlib creates the host_name, kv-nnnnn-xxxxxx, on supported devices, where nn is lower part of EAN number and xx is serial number. KvrLib will remove leading and trailing dashes. Space is replaced with dash ('-'), any characters except dash, a-z and 0-9 are discarded and everything is converted to lowercase. The resulting host_name must contain at least one token to be valid.

ssid	xml string	The name of the network that the Kvaser BlackBird will try to connect to. Maximum ssid length is 32 characters. The actual restriction is device dependent and not verified in the XML. It is strongly recommended to only use ASCII characters in the range 0x20-0x7E.
operation_mode	INFRASTRUCTURE ADHOC	The network module used by the Kvaser BlackBird.
search_all_channels	YES / NO	Enable search_all_channels to make the Kvaser BlackBird search for a network channel given the SSID.
channel	1, 2, ... 14	The channel the Kvaser BlackBird will use when trying to connectd to the network. In AdHoc mode with search_all_channels enabled, the selected channel will be used to start a new network if the specified SSID cannot be found. Not used in infrastructure mode if search_all_channels is enabled.
port	11416	Port used for UDP broadcast messages and TCP/IP traffic.
mtu	576-1500	Maximum transmission unit (optional, device dependent default).

Table 5: Attributes for element NETWORK

2.7 Profile Info (PROFILE_INFO)

This element defines the name of the profile.

Element name: `PROFILE_INFO`
Children: `None`

```
<!-- Profile Name -->
<PROFILE_INFO
  name="Name Of The Profile"
/>
```

Attribute name	Value	Description
name	xml string	The name of the profile. Maximum length is 32 characters.

Table 6: Attributes for element PROFILE_INFO

2.8 Security Settings (NETWORK_SECURITY)

This element contains attributes `key` and `passphrase` that are syntactically not mandatory, but they might be needed anyway. If either `key` or `passphrase` is not included in the XML when writing a new configuration to a device, the old `key` or

`passphrase` will be used *if the device supports this functionality*; otherwise an error will occur. It is not allowed to have both `key` and `passphrase` at the same time.

Element name: `NETWORK_SECURITY`
Children: `WPA_WPA2` or `WEP64_WEP128`

```
<!-- Security/encryption setting for WPA2 -->
<NETWORK_SECURITY
  encryption_mode="WPA2">
  <WPA_WPA2
    group_encryption="AES"
    pairwise_encryption="AES"
    passphrase="SecretPassphrase"
  />
</NETWORK_SECURITY>
```

Attribute name	Value	Description
encryption_mode	OPEN	No encryption.
	WEP64	WEP encryption with 64 bit key length.
	WEP128	WEP encryption with 128 bit key length.
	WPA	Wi-Fi Protected Access.
	WPA2	Wi-Fi Protected Access II.

Table 7: Attributes for element NETWORK_SECURITY

2.8.1 WPA (WPA_WPA2)

Select authentication and encryption keys for Wi-Fi Protected Access (WPA). The element `NETWORK_SECURITY` selects between WPA and WPA2.

Element name: `WPA_WPA2`
Children: `None`

```
<!-- Network security setting for WPA using passphrase -->
<WPA_WPA2
  group_encryption="TKIP"
  pairwise_encryption="TKIP"
  passphrase="SecretPassphrase"
/>

<!-- Network security setting for WPA using key -->
<WPA_WPA2
  group_encryption="TKIP"
  pairwise_encryption="TKIP"
  key="1234567890ABCDEF12345678901234567890ABCDEF12345678901234567890AB"
/>
```

Attribute name	Value	Description
group_encryption	TKIP	Temporal Key Integrity Protocol is recommended for WPA.
	AES	Advanced Encryption Standard is recommended for WPA2.
pairwise_encryption	TKIP	Temporal Key Integrity Protocol is recommended for WPA.
	AES	Advanced Encryption Standard is recommended for WPA2.
passphrase	xml string	WPA/WPA2 passphrase as a string of max 63 characters. The passphrase may only include ASCII characters in the range 32 to 126 (decimal), inclusive.
key	hexadecimal string	WPA key as string of 64 hexadecimal characters (256 bits).

Table 8: Attributes for element WPA_WPA2

Note: For access points allowing simultaneous WPA and WPA2, the following settings are recommended.

```
<!-- Network security setting for simultaneous WPA and WPA2 using passphrase -->
<NETWORK_SECURITY
  encryption_mode="WPA2">
  <WPA_WPA2
    group_encryption="TKIP"
    pairwise_encryption="AES"
    passphrase="SecretPassphrase"
  />
</NETWORK_SECURITY>

<!-- Network security setting for simultaneous WPA and WPA2 using key -->
<NETWORK_SECURITY
  encryption_mode="WPA2">
  <WPA_WPA2
    group_encryption="TKIP"
    pairwise_encryption="AES"
    key="1234567890ABCDEF1234567890123456789012345678901234567890AB"
  />
</NETWORK_SECURITY>
```

2.8.2 WEP (WEP64_WEP128)

Select authentication and encryption keys for Wired Equivalent Privacy (WEP). The element `NETWORK_SECURITY` selects between WEP64 and WEP128.

Element name: `WEP64_WEP128`
Children: `None`

```
<!-- Network security setting for WEP128 using passphrase -->
<WEP64_WEP128
  authentication_type="OPEN"
  active_key="1"
  passphrase="SecretPassphrase"
/>

<!-- Network security setting for WEP128 using keys -->
<WEP64_WEP128
  authentication_type="OPEN"
  active_key="1"
  key1="1234567890ABCDEF1234567890"
  key2="1234567890ABCDEF1234567890"
  key3="1234567890ABCDEF1234567890"
  key4="1234567890ABCDEF1234567890"
/>
```

Attribute name	Value	Description
authentication_type	OPEN	Open System authentication.
	SHARED_KEY	Shared Key authentication.
active_key	1,2,3,4	Specify which one of the WEP keys to use. Should normally be set to 1.
passphrase	xml string	WEP passphrase as a string of max 63 characters. The passphrase may only include ASCII characters in the range 32 to 126 (decimal), inclusive.
key1	hexadecimal string	WEP64 key as string of 10 hexadecimal characters. WEP128 key as string of 26 hexadecimal characters.
key2	hexadecimal string	See key1.
key3	hexadecimal string	See key1.
key4	hexadecimal string	See key1.

Table 9: Attributes for element WEP64_WEP128

2.9 Traffic Encryption Settings (TRAFFIC_ENCRYPTION)

Select traffic encryption type for a device. This element is not mandatory and the default setting is to not encrypt the communication.

Element name: `TRAFFIC_ENCRYPTTION`
Children: `None`

```
<!-- Encrypt traffic with RC4 -->
<TRAFFIC_ENCRYPTION
  type="RC4"
  key="asdf2011"
/>
```

Attribute name	Value	Description
type	NONE	No encryption.
	RC4	Encrypt traffic with RC4.
key	xml string	Maximum passpassword length is 31 characters. The communication will be encrypted even if key is empty (i.e. if the length of the password string is 0).

Table 10: Attributes for element TRAFFIC_ENCRYPTION

2.10 Web Server (WEBSERVER)

Settings for the internal web server in the Kvaser BlackBird. (On supported devices only.)

Element name: `WEBSERVER`
Children: `None`

```
<!-- Enable the webserver -->
<WEBSERVER
  enabled="YES"
  change_log_settings="NO"
  user_data_download="NO"
  debug_commands="NO"
/>
```

Attribute name	Value	Description
enabled	YES / NO	Enables the internal webserver in the device.
change_log_settings	YES / NO	Allows users to change the log settings.
user_data_download	YES / NO	Allows users to download data to the webserver.
debug_commands	YES / NO	Enables debug commands.

Table 11: Attributes for element WEBSERVER

2.11 Region Settings (REGION_SETTINGS)

Region settings to control the radio transmission power of the Kvaser BlackBird.

Element name: `REGION_SETTINGS`
Children: `None`

```
<REGION_SETTINGS
  regulatory_domain="WORLD"
/>
```

Attribute name	Value	Description
regulatory_domain	WORLD EUROPE_ETSI NORTH_AMERICA_FCC JAPAN_TELEC CHINA_MII	The geographical region where the Kvaser BlackBird will be operated must be selected here. It might not be legal to select a different region than the region of operation. If your country isn't listed, please check with your local government.

Table 12: Attributes for element REGION_SETTINGS

2.12 Roaming Settings (ROAMING_SETTINGS)

Select roaming settings for a device. This element is not mandatory, but skipping it enforces default settings (which are device-specific).

Element name: `ROAMING_SETTINGS`
Children: `None`

```
<!-- Roam on channels 1, 6, 11 if signal is -75dBm or worse-->
<ROAMING_SETTINGS
  channels="1057"
  threshold="75"
/>
```

Attribute name	Value	Description
channels	integer	Binary channel mask written in decimal format, where least significant bit stands for channel 1
threshold	integer 0..100	Signal strength in -dBm, at which device will consider roaming alternatives

Table 13: Attributes for element TRAFFIC_ENCRYPTION

3 Version History

Version history for document SP_98100_xml_format:

Revision	Date	Changes
-	2011-02-23	Preliminary revision.
2.0	2011-09-06	Added encrypted_password to <DEVICE_ACCESS>.
3.0	2011-10-12	Increased XML version to 3.0. Added information about reserved characters in XML.
4.0	2011-12-12	Passphrases is now used instead of keys for WEP, WPA, & WPA2. Traffic encryption attribute "mode" is now called "type". Updated Sample XML configuration. <SECURITY> is now called <NETWORK_SECURITY>. Increased XML version to 4.0. Removed encrypted password from <DEVICE_ACCESS>. Added a footnote about hostname and valid characters in xml strings. Changed maximum SSID length from 31 to 32.
4.1	2012-01-16	Added keys as an alternative to passphrase when setting up WEP, WPA, and WPA2. Either key or passphrase can be used but not both at the same time.
4.2	2012-05-14	Added <PROFILE_INFO>. Removed default columns from tables. Updated Sample with mandatory entries.
4.3	2012-08-20	Added description for optional host_name. Added recommendation for ssid.
4.3	2014-01-12	Added information about Kvaser Ethercan. Renamed document. Changed layout of references, figures. Changed footnote description for optional host_name. Clarified webserver only on supported devices.Converted to LaTeX.
4.4	2014-04-03	Corrected XML version to 4.3.
4.5	2014-04-15	Renumbered pages.
4.6	2014-09-11	Removed information about Kvaser Ethercan.
4.7	2015-05-12	Added description for roaming settings.
4.8	2018-06-25	Updated device list.

4 Appendix

4.1 Sample XML Configuration

```
<?xml version="1.0" encoding="ISO-8859-1"?>

<KVASER>
  <!-- Version is the version of the XML format -->
  <VERSION>4.3</VERSION>
  <PRODUCTFAMILY>Blackbird</PRODUCTFAMILY>

  <!-- Allow any user to see and access the BlackBird -->
  <DEVICE_ACCESS
    level="PUBLIC"
    password=""
  />

  <!-- The protect the configuration with a password -->
  <CONFIG_PROTECTION
    protected="YES"
    password="qwerty12"
  />

  <!-- Infrastructure mode with DHCP -->
  <NETWORK
    ssid="MyNetwork"
    operation_mode="INFRASTRUCTURE"
    channel="6"
    search_all_channels="NO"
    device_name="Blackbird#42"
    address_type="DHCP"
    port="11416"
  />

  <!-- Roam on channels 1, 6, 11 if signal is 75 or worse-->
  <ROAMING_SETTINGS
    channels="1057"
    threshold="75"
  />

  <!-- Profile Name -->
  <PROFILE_INFO
    name="Name Of The Profile"
  />
```

```
  <!-- Use WPA2/TKIP -->
  <NETWORK_SECURITY
    encryption_mode="WPA2">
    <WPA_WPA2
      group_encryption="TKIP"
      pairwise_encryption="AES"
      passphrase="SecretPassphrase"
    />
  </NETWORK_SECURITY>

  <!-- Encrypt traffic with RC4 -->
  <TRAFFIC_ENCRYPTION
    type="RC4"
    key="asdf2011"
  />

  <!-- Disable the internal web server -->
  <WEBSERVER
    enabled="NO"
    change_log_settings="NO"
    user_data_download="NO"
    debug_commands="NO"
  />

  <!-- The geographical region -->
  <REGION_SETTINGS
    regulatory_domain="WORLD"
  />

</KVASER>
```