Technische Spezifikation

Anforderungen an Systemhersteller

ENERCON Bedarfsgerechte Nachtkennzeichnung (BNK)

ENERCON
ENERGIE FÜR DIE WELT

Herausgeber

ENERCON GmbH ▪ Dreekamp 5 ▪ 26605 Aurich ▪ Deutschland
Telefon: +49 4941 927-0 ▪ Telefax: +49 4941 927-109
E-Mail: info@enercon.de ▪ Internet: http://www.enercon.de
Geschäftsführer: Momme Janssen, Jost Backhaus, Stefan Lütkemeyer, Dr. Martin Prillmann, Jörg Scholle
Zuständiges Amtsgericht: Aurich ▪ Handelsregisternummer: HRB 411
Ust.Id.-Nr.: DE 181 977 360

Dokumentinformation

Dokument-ID	D0611773/1.1-de
Vermerk	Originaldokument

Datum	**Sprache**	**DCC**	**Werk / Abteilung**
2020-12-07	de	EC	WRD Management Support GmbH / Technische Redaktion

Inhaltsverzeichnis

1 Einleitung 5

2 Funktionale Anforderungen 5

3 Schnittstellendefinition 6

4 TLS-Kommunikation 8

4.1 Funktion 8

4.2 Konfiguration 10

4.3 Zertifikatsvalidierung 11

4.4 Zertifikatsinfrastruktur 12

Abkürzungsverzeichnis

ASCII	American Standard Code for Information Interchange (amerikanischer Standard-Code für Informationsaustausch)
AVV	Allgemeine Verwaltungsvorschrift
BCMT	Begin of civil morning twilight (Beginn der bürgerlichen Morgendämmerung)
BNK	Bedarfsgerechte Nachtkennzeichnung
BSI	Bundesamt für Sicherheit in der Informationstechnik
CA	Certificate authority (Zertifizierungsstelle)
CN	Common name (gemeinsamer Name)
CRC	Cyclic redundancy check (zyklische Redundanzprüfung)
CRL	Certificate revocation list (Zertifikatsperrliste)
ECET	End of civil evening twilight (Ende der bürgerlichen Abenddämmerung)
EPK	ENERCON PartnerKonzept
HMAC	Keyed-hash message authentication code (hashbasierte, schlüsselabhängige kryptographische Prüfsumme)
PKI	Public key infrastructure (Sicherheitsinfrastruktur mit öffentlich hinterlegtem Schlüssel)
SSL	Secure Sockets Layer (Netzwerkprotokoll zur sicheren Datenübertragung)
TLS	Transport Layer Security (Netzwerkprotokoll zur sicheren Datenübertragung)
URL	Uniform Resource Locator (eindeutige Adresse innerhalb eines Computernetzwerks)

1 Einleitung

Zur bedarfsgerechten Steuerung der Nachtkennzeichnung von ENERCON Windenergieanlagen über die ENERCON SCADA BNK-Schnittstelle muss das steuernde System die in diesem Dokument aufgeführten Anforderungen erfüllen.

2 Funktionale Anforderungen

Umsetzung nach AVV

Grundlage für die Umsetzung der bedarfsgerechten Nachtkennzeichnung ist die zum jeweiligen Zeitpunkt gültige Allgemeine Verwaltungsvorschrift zur Kennzeichnung von Luftfahrthindernissen. Insbesondere in Anhang 6 wird auf die Funktion der bedarfsgerechten Nachtkennzeichnung von Windenergieanlagen eingegangen. Des Weiteren sind folgende Anforderungen zu erfüllen:

Tab. 1: Funktionale Anforderungen

ID	Anforderung	Kriterium	Verantwortlichkeit	
			ENERCON	Systemhersteller
BNK01	Ein Betrieb der Befeuerung außerhalb der Zeit von ECET und BCMT ist durch einen Dämmerungsschalter zu gewährleisten. BNK inaktiv → autonomer Betrieb der Befeuerung Dies ist durch das verteilte BNK-Signal sicherzustellen. BNK → SCADA → Windenergieanlage → Befeuerung	muss	X	
BNK02	Die Nachtkennzeichnung darf abgeschaltet werden, wenn sich kein relevantes Luftfahrzeug im Wirkungsraum befindet. (gewünschte Funktion von BNK)	muss		X
BNK03	Die Nachtkennzeichnung darf abgeschaltet werden, wenn die Systemintegrität sowie eine ausreichende Detektionsleistung durch die Selbstdiagnose signalisiert werden (ordnungsgemäßer Betrieb, kein Fehler). Ein Fehler einer Komponente → alle Leuchten an Signal: Fehler/kein Fehler an SCADA	muss		X
BNK04	Wenn die Bedingungen für ein Abschalten der Befeuerung nicht erfüllt sind, ist die gesamte Befeuerung sofort in Betrieb zu	muss		X

ID	Anforderung	Kriterium	Verantwortlichkeit	
			ENERCON	Systemhersteller
	versetzen (100 % Nennlichtstärke).			
BNK05	Das Gesamtsystem BNK muss durch eine durch das Bundesministerium für Verkehr und digitale Infrastruktur benannte Stelle anerkannt sein.	muss	X	X
BNK06	Überwachung der Paketlaufzeit anhand der Antwort des SCADA Systems	muss		X
BNK07	RJ45 zur Anbindung BNK an das SCADA System	muss	X	X

Tab. 2: Allgemeine Anforderungen

Allgemeine Anforderungen				
A01	90 % Jahresverfügbarkeit des BNK-Systems (System und Kommunikation zum Windpark) Die Betreuung muss den Bedingungen eines EPK-Vertrags unterliegen.	muss	X	X
A02	Einhaltung des IT-Sicherheitsgesetzes unter dem Gesichtspunkt kritischer Infrastrukturen	muss	X	X

3 Schnittstellendefinition

Die Schnittstelle zwischen dem BNK-System und dem ENERCON SCADA System wird bidirektional ausgeführt. Basis hierbei ist eine TCP-Socket-Verbindung, die mit TLS ausgeführt wird. Die Authentifizierung und Autorisierung erfolgt zertifikatbasiert. Um die Latenz in der Kommunikation so klein wie möglich zu halten, muss hier mit einer etablierten Socket-Verbindung (d. h. ohne ständigen Verbindungsauf- und -abbau) gearbeitet werden.

Daten vom BNK-System an das ENERCON SCADA System

Zur Steuerung der Befeuerung müssen Informationen vom BNK-System an das ENERCON SCADA System übertragen werden. Dabei müssen die folgenden Eigenschaften beachtet werden:

- Byte-Reihenfolge: Big-Endian
- Zykluszeit: 1,5 Sekunden
- Timeout: 4,5 Sekunden

Der durch das BNK-System überwachte Luftraum muss um die Strecke erweitert werden, die ein Luftfahrzeug innerhalb des Timeouts zurücklegt.

Tab. 3: Steuerdatensatz

Byte-Nr.	Bit-Nr.	Information	Gültige Werte			Ungültige Werte
0	0-7	Versionsnummer (SCADA-Schnittstelle)	1			Sonstige
1	8-15	eindeutiger Paket-Identifier	0x42 (ASCII-Code für "B")			Sonstige
2	16-23	lfd. Paketnummer	0-255			-
3	24	Befeuerung unterdrücken	0: Befeuerung nicht unterdrücken 1: Befeuerung unterdrücken			-
3	25	aktiver BNK-Betrieb	0: passiver BNK-Betrieb; Befeuerung soll nicht bedarfsgerecht gesteuert werden (z. B. außerhalb des zulässigen Zeitfensters) 1: aktiver BNK-Betrieb; Befeuerung soll bedarfsgerecht gesteuert werden (z. B. innerhalb des zulässigen Zeitfensters)			-
3	26	Fehler des BNK-Systems (z. B. keine verlässliche Detektion möglich)	0: kein Fehler 1: Fehler			-
3	27-28	Startsequenz der Befeuerung	Bit 28	Bit 27	Variante	11
			0	0	A	
			0	1	B	
			1	0	C	
3	29-31	nicht verwendet	000			Sonstige
4-6	32-55	CRC-Prüfsumme (über die Bytes 1-3; ohne Versionsnummer in Byte 0)	-			-

Spezifikation der CRC-Berechnungsmethode

- Polynom: 0xCBA785
- Grad des Polynoms: 24
- Initialwert: 0xFFFFFF
- Wert für finales XOR: 0xFFFFFF
- non-direct

Daten vom ENERCON SCADA System an das BNK-System

Das ENERCON SCADA System antwortet umgehend auf eingehende BNK-Informationen. Dabei muss die folgende Eigenschaft beachtet werden:

- Byte-Reihenfolge: Big-Endian

Tab. 4: Antwortdatensatz

Byte-Nr.	Information	Gültige Werte	Ungültige Werte
0	Versionsnummer	1	Sonstige
1-6	gespiegelte Daten vom BNK-System	siehe Steuerdatensatz des BNK-Systems (Byte 1-6)	
7-8	aktuelles Jahr vom SCADA System	0-65535	-
9	aktueller Monat vom SCADA System	1-12	Sonstige
10	aktueller Tag vom SCADA System	1-31	Sonstige
11	aktuelle Stunde vom SCADA System	0-23	Sonstige
12	aktuelle Minute vom SCADA System	0-59	Sonstige
13	aktuelle Sekunde vom SCADA System	0-59	Sonstige
14	Anzahl vorhandener Windenergieanlagen im Windpark	0-255	-
15	Anzahl der Windenergieanlagen mit Kommunikationsstörungen	0-255	-
16	Anzahl der Windenergieanlagen mit gestörter Befeuerung	0-255	-

4 TLS-Kommunikation

4.1 Funktion

Zwischen dem ENERCON SCADA System in der Rolle als Server und einem BNK-System in der Rolle als Client wird eine TLS-gesicherte Kommunikation etabliert. Zur gegenseitigen Authentifizierung werden X509-Zertifikate eingesetzt, welche aus der ENERCON SCADA-PKI abgeleitet sind.

Die ENERCON SCADA-PKI besteht aus der Root-CA mit dem CommonName (CN) „EC2-SCADACA-1“ sowie der Intermediate-CA für Kommunikationsstrukturen mit dem CN „EC2-CommCA-1“. Aussteller der Server- bzw. Client-Zertifikate ist die Intermediate-CA.

Jedes X509-Zertifikat dient als eindeutiges Identifizierungsmerkmal und Authentifizierungsmerkmal und darf nur in einem System verwendet werden. Der im Zertifikat hinterlegte CN muss eindeutig sein und einen exakten Rückschluss auf das verwendete System ermöglichen (Beispiel SCADA: Der CN „SCADA_1234“ beschreibt das SCADA-Server-Zertifikat eines Windparks mit der Windpark-ID 1234).

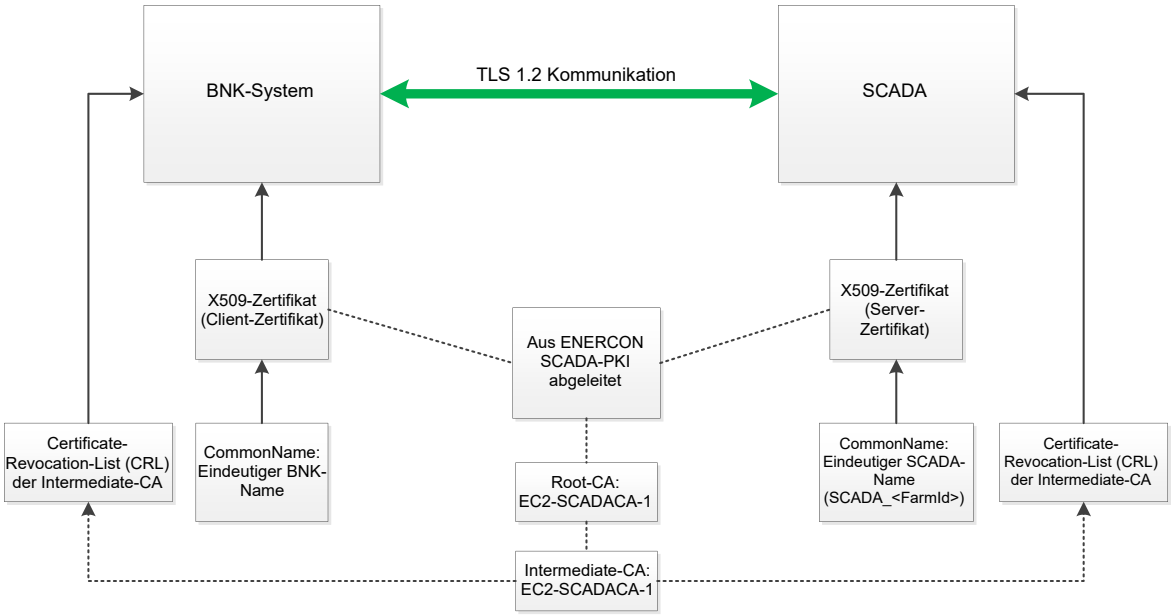

Abb. 1: Übersicht TLS

Bei einem Austausch oder einer Kompromittierung des Systems wird das verknüpfte X509-Zertifikat durch die Intermediate-CA zurückgerufen. Hierzu wird in regelmäßigen Abständen eine Certificate-Revocation-List (CRL) erstellt und veröffentlicht.

Alle an einer TLS-Kommunikation teilnehmenden Systeme müssen diese CRL regelmäßig aktualisieren und validieren.

4.2 Konfiguration

Die Konfiguration der TLS-Kommunikation basiert auf der technischen Richtlinie TR-02102-2 (Version 2017-01) vom Bundesamt für Sicherheit in der Informationstechnik (BSI) über die Verwendung von Transport Layer Security (TLS).

Der ENERCON SCADA Server unterstützt folgende Konfigurationen:

- SSL /TLS-Version: TLS 1.2 (nicht abwärtskompatibel zu älteren Versionen)
- elliptische Kurven: secp256r1, secp384r1
- Cipher Suites:

TLS_	ECDHE_RSA_	WITH_	AES_128_	CBC_	SHA256
				GCM_	
			AES_256_	CBC_	SHA384
				GCM_	
	ECDH_RSA_		AES_128_	CBC_	SHA256
				GCM_	
			AES_256_	CBC_	SHA384
				GCM_	

- Cipher-Suites mit Pre-Shared Key werden grundsätzlich nicht unterstützt.
- weitere Optionen:
  - Session Renegotiation darf nicht unterstützt/verwendet werden.
  - Kompression muss deaktiviert sein.
  - Verkürzung der HMAC-Ausgabe (truncated_hmac) darf nicht unterstützt/verwendet werden.
  - Heartbeat-Erweiterung darf nicht unterstützt/verwendet werden.

4.3 Zertifikatsvalidierung

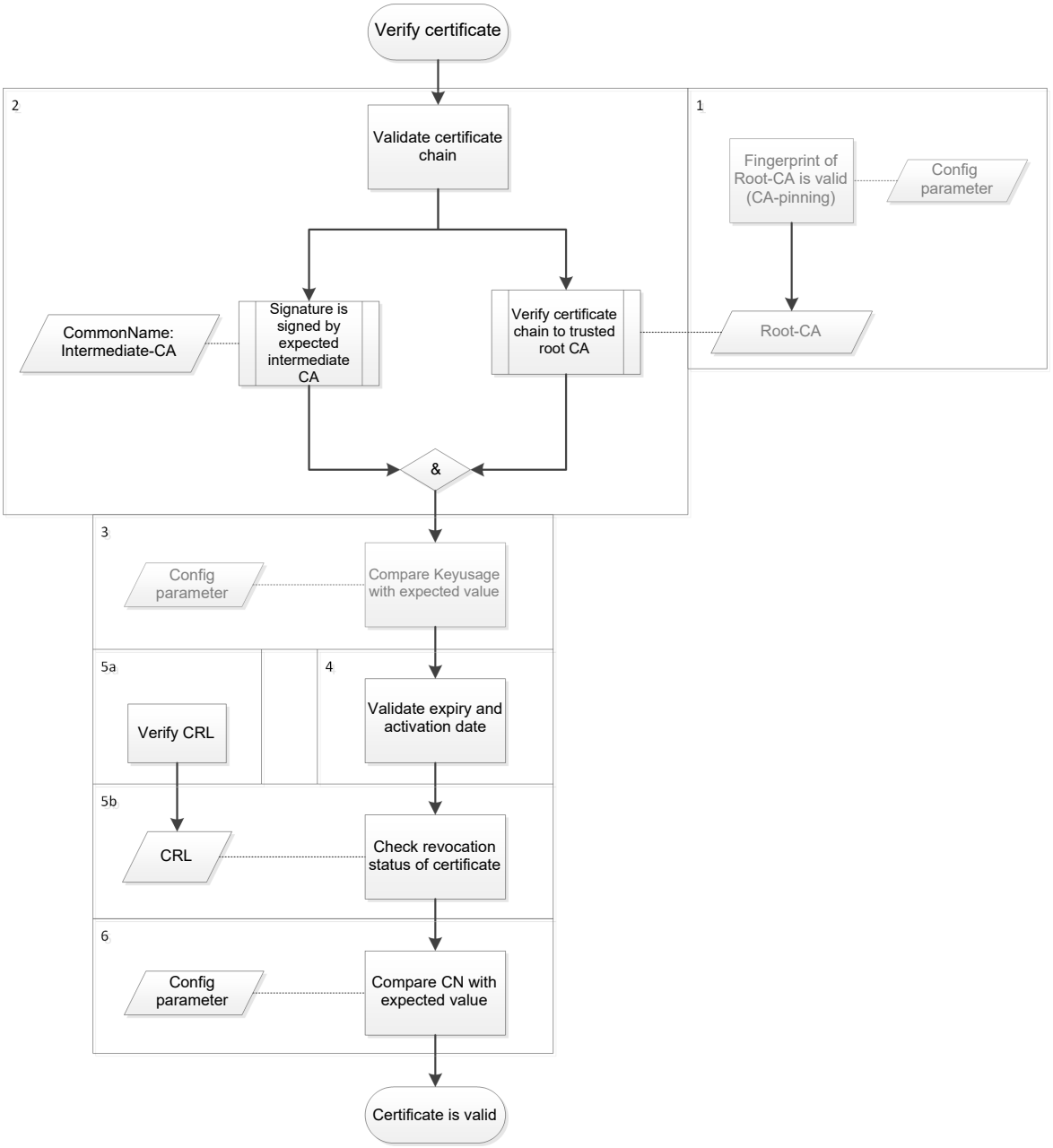

Abb. 2: Zertifikatsvalidierung

Die Validierung des Zertifikats des Kommunikationspartners wird wie folgt umgesetzt:

Tab. 5: Schritte der Zertifikatsvalidierung

Schritt	Beschreibung
1	(Optional) Das Root-CA-Zertifikat sollte grundsätzlich bereits auf dem System vorhanden sein. Wird das Root-CA-Zertifikat nicht in einem vertrauenswürdigen Zertifikatsspeicher vorgehalten, kann eine zusätzliche Überprüfung des Fingerprints durchgeführt werden, um einen potenziellen Austausch bzw. eine Kompromittierung auszuschließen. Bei Erfolg wird die Root-CA als Vertrauensanker der gesamten Kommunikation angesehen. Der Fingerprint sollte zwecks Root-CA-Wechsel konfigurierbar sein.

Schritt	Beschreibung
2	Die Überprüfung der Zertifikatskette (certificate chain) ist in zwei Teilbereiche aufgeteilt.
2a	Im ersten Schritt wird die gesamte Kette bis zum Vertrauensanker (Root-CA) verifiziert.
2b	Zusätzlich wird überprüft, ob das Zertifikat von der erwarteten Intermediate-CA (für TLS-Verbindungen die „EC2-CommCA-1“) ausgestellt wurde. Der hierfür erforderliche CN der Intermediate-CA sollte als konfigurierbarer Parameter vorgehalten werden.
3	(Optional) Im nächsten Schritt kann zusätzlich die im Zertifikat hinterlegte Schlüsselverwendung „Key usage“ anhand eines Erwartungswertes überprüft werden.
4	In jedem Zertifikat ist eine Gültigkeitsdauer durch ein Start- und ein End-Datum angegeben, wobei die aktuelle Zeit (Systemzeit) innerhalb dieses Fensters liegen muss.
5	Um den Widerrufstatus eines Zertifikats überprüfen zu können, wird durch die ENERCON SCADA-PKI eine CRL bereitgestellt. In jedem Zertifikat ist hinterlegt, unter welchen Adressen (URL) die aktuelle CRL bezogen werden kann.
5a	Wird eine neue CRL initialisiert, müssen die Signatur sowie die Gültigkeitsdaten überprüft werden.
5b	Auf Basis dieser CRL wird dann für jedes Zertifikat während des Kommunikationsaufbaus überprüft, ob ein Zertifikat zurückgezogen wurde. Sollte keine aktuelle CRL vorliegen, wird der Widerrufstatus (RevocationStatus) zur Aufrechterhaltung einer funktionierenden Kommunikation ignoriert. In diesem Fall soll jedoch eine entsprechende Alarm-Meldung generiert werden.
6	Abschließend wird der im Zertifikat hinterlegte CN mit dem erwarteten Wert verglichen. Der erwartete CN sollte als konfigurierbarer Parameter hinterlegt werden.

4.4 Zertifikatsinfrastruktur

Für eine funktionierende Zertifikatsinfrastruktur müssen durch alle Systeme zwei wesentliche Prozesse unterstützt werden:

Zertifikatswechsel

Üblicherweise haben Zertifikate aus der ENERCON SCADA-PKI eine Gültigkeitsdauer von fünf Jahren. Aus diesem Grund muss es einen Prozess bzw. ein Verfahren geben, um ein Zertifikat auszutauschen, wobei das ausgetauschte Zertifikat aus derselben Zertifikatskette abgeleitet wird.

Root-CA-Wechsel

Die Gültigkeitsdauer des Root-CA-Zertifikats ist wesentlich länger, jedoch nicht unbegrenzt. Aus diesem Grund muss es einen Prozess bzw. ein Verfahren geben, um das Stammzertifikat auszutauschen. Üblicherweise wird das Vertrauen zu einer neuen Root-CA über eine Kreuzsignierung zwischen alter und neuer Root-CA hergestellt, weshalb für einen begrenzten Zeitraum mindestens zwei Stammzertifikate gültig sein können.