SecureD v.1.6.1 Security Policy

Document Number: SecureD Security Policy – 100502DS – 02.00

Information Grade: Non-Proprietary

Effective Date: 2005-01-10

Updated: 2006-11-01

High Density Devices AS

Ballastgata 9

PO Box 1428

N-4505 Mandal, Norway

Document Revision History

Revision	Date	Author	Notes	MR#
00.50	2004-09-30	Alan Dowd	First Edition	
00.50	2004-10-22	Tormod Fjellgård	Formatted document to suit HDD Document Template	
00.50	2004-11-25	Tormod Fjellgård	Revised document	
00.50	2005-01-05	Tormod Fjellgård	Revised document	
00.50	2005-01-05	Alan Dowd	Review comments	
00.50	2005-01-07	Tormod Fjellgård	Revised document	
00.50	2005-01-10	Atle Haga	Commented and revised document	
01.00	2005-01-10	TF, AH, JE	Document Reviewed and Approved	
01.00	2005-02-04	Tormod Fjellgård	Revised document after InfoGard Review	
01.10	2005-02-04	TF, AH, JE	Document Reviewed and Approved	
01.10	2005-02-16	Tormod Fjellgård	Revised document after InfoGard Review	
01.20	2005-02-17	TF, AH, JE	Document Reviewed and Approved	
01.30	2005-02-23	Tormod Fjellgård	Changed document number	MR#78
01.40	2005-05-12	TF, AH, SA, JE, AV	Document review after Operational Testing	MR#111
01.40	2005-05-20	Tormod Fjellgård	Document formatted for delivery to InfoGard	MR#111
01.50	2005-06-27	TF, SA, JE	InfoGard changes modified and accepted over telephone, document formatted and returned	MR#145
01.60	2005-08-05	TF, SA, JE	InfoGard changes reviewed and approved	MR#159
01.70	2005-11-07	Tormod Fjellgård	Document revised after NIST comments	MR#204
01.80	2006-02-14	TF, JE	Document Reviewed for LX25-evaluation	MR#243
01.90	2006-03-07	Tormod Fjellgård	Revision after FIPS evaluation	MR#282
01.90	2006-06-15	Tormod Fjellgård	Reviewed and approved evaluator changes	
02.00	2006-11-01	Tormod Fjellgård	Reviewed and approved validator changes	

Trademark Disclaimers

High Density Devices AS, Postboks 1428, N-4505 Mandal, Norway
Phone: +47 38 27 25 20 Fax: +47 38 27 25 49
Org.Nr: NO 980 447 146 MVA

Contents

High Density Devices AS, Postboks 1428, N-4505 Mandal, Norway
Phone: +47 38 27 25 20 Fax: +47 38 27 25 49
Org.Nr: NO 980 447 146 MVA

Tables

Figures

High Density Devices AS, Postboks 1428, N-4505 Mandal, Norway
Phone: +47 38 27 25 20 Fax: +47 38 27 25 49
Org.Nr: NO 980 447 146 MVA

References

This Security Policy refers to the following documents and incorporates them by reference:

#	Document Title	Additional Information
1	Advanced Encryption Standard (AES)	FIPS Publication 197. National Institute of Standards and Technology, November 2001
2	Recommendation for Block Cipher Modes of Operation - Methods and Techniques	Special Publication 800-38A, 2001 Edition. National Institute of Standards and Technology, December 2001
3	Security Requirements for Cryptographic Modules	FIPS Publication 140-2, National Institute of Standards and Technology, May 2001
4	Derived Test Requirements for FIPS PUB 140-2, Security Requirements for Cryptographic Modules	National Institute of Standards and Technology, March 24, 2004 DRAFT
5	Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher	Special Publication 800-67, National Institute of Standards and Technology, March 2004

Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
CBC	Cipher Block Chaining
CSP	Critical Security Parameters
EDC	Error Detection Code
TDEA	Triple Data Encryption Algorithm

High Density Devices AS, Postboks 1428, N-4505 Mandal, Norway
Phone: +47 38 27 25 20 Fax: +47 38 27 25 49
Org.Nr: NO 980 447 146 MVA

1 Module Overview

The SecureD data storage encryption device (SecureD) v.1.6.1 is a fully ATA / ATAPI-6 (IDE) compatible hardware encryption device that resides in the data path between an IDE controller and IDE devices in a general computing environment. It applies Advanced Encryption Standard (AES) encryption at the sector level to protect data at rest from intentional or inadvertent disclosure. SecureD loads its cryptographic keys from an external Key Token – typically a smart card – through an encrypted external interface, logically and physically separate from the data path. SecureD supports multiple key lengths (128, 192, and 256 bits) and up to 32 different keys per user. Each key can be allocated any non-overlapping sector range on the storage medium. SecureD incorporates a hardware function for zeroizing the keys controlled by an external pin for connection to tamper-detection circuitry. SecureD is encapsulated in a hard, opaque, tamper-evident coating. The validated version of SecureD is SecureD version 1.6.1, Hardware version 1.6.6 and Firmware version 1.6.3 and is a multi-chip embedded module.

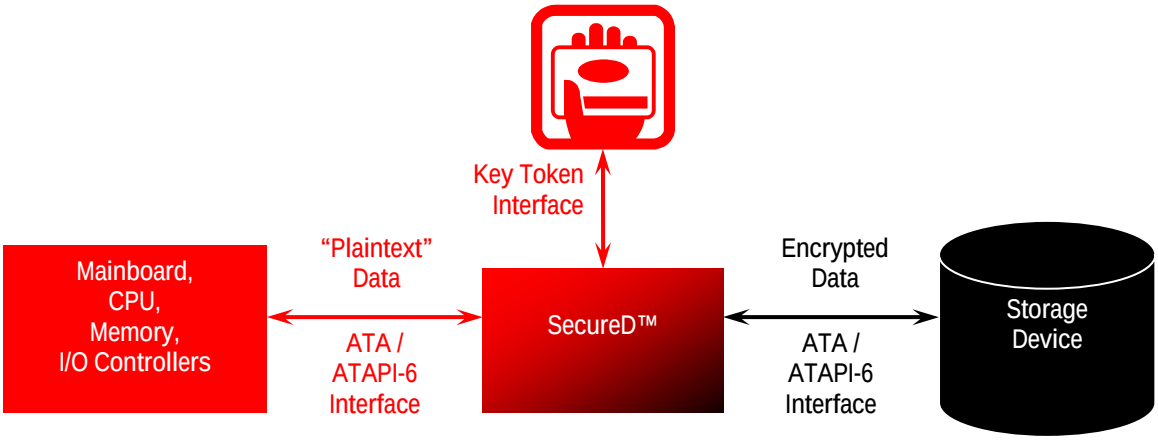

Figure 1 The SecureD data storage solution

High Density Devices AS, Postboks 1428, N-4505 Mandal, Norway
Phone: +47 38 27 25 20 Fax: +47 38 27 25 49
Org.Nr: NO 980 447 146 MVA

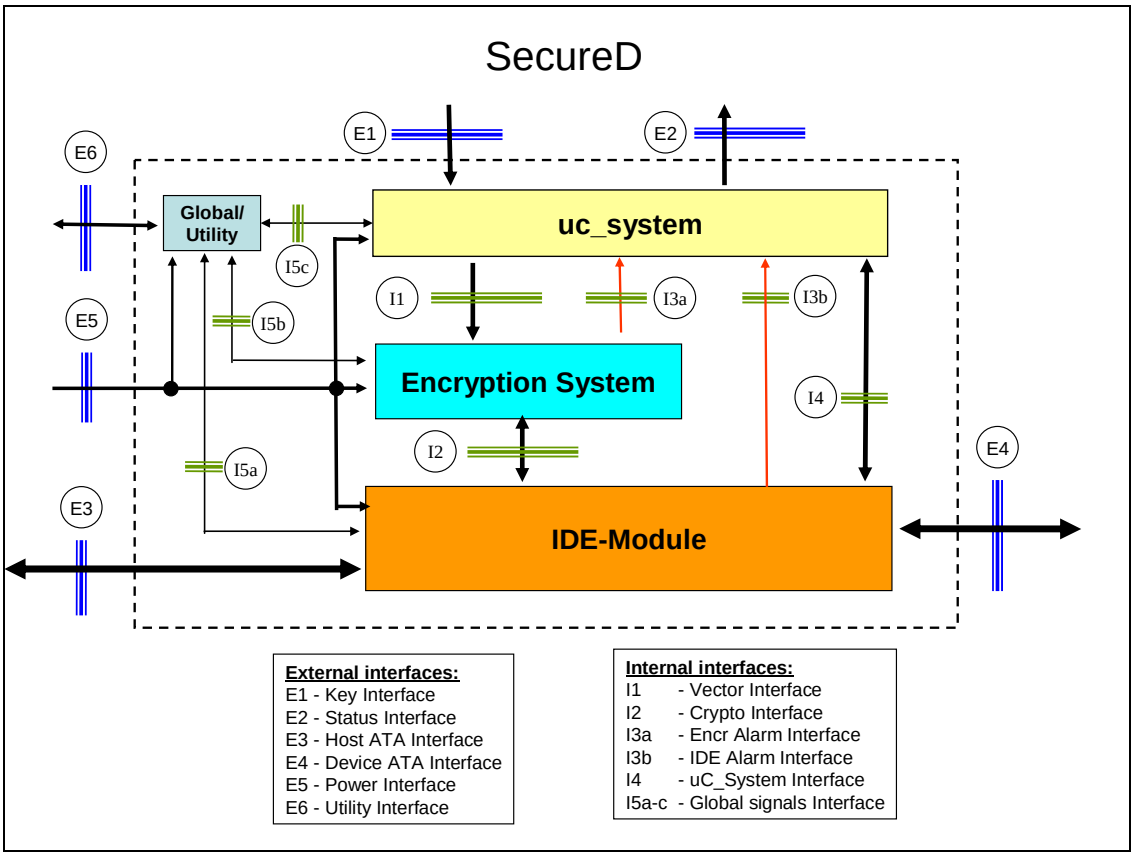

Figure 2 SecureD Modules – Conceptual Model

Figure 3 SecureD FPGA Sample (front)
– Epoxy Coated with Tamper Sticker Sample

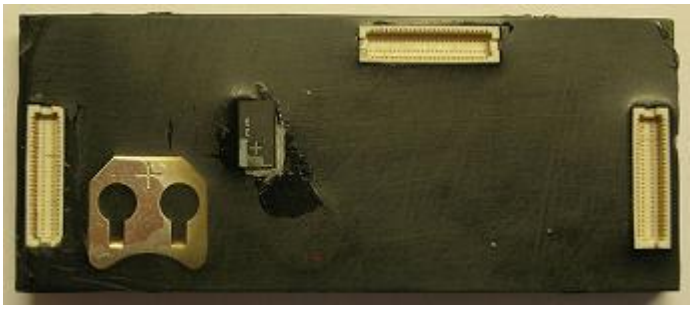

Figure 4 SecureD FPGA Sample (back)
– Epoxy Coated

High Density Devices AS, Postboks 1428, N-4505 Mandal, Norway
Phone: +47 38 27 25 20 Fax: +47 38 27 25 49
Org.Nr: NO 980 447 146 MVA

2 Security Level

The cryptographic module meets the overall requirements applicable to Level 3 security of FIPS 140-2.

Table 1 Module Security Level Specification

Security Requirements Section	Level
Cryptographic Module Specification	3
Module Ports and Interfaces	3
Roles, Services and Authentication	3
Finite State Model	3
Physical Security	3
Operational Environment	N/A
Cryptographic Key Management	3
EMI/EMC	3
Self Test	3
Design Assurance	3
Mitigation of Other Attacks	N/A

High Density Devices AS, Postboks 1428, N-4505 Mandal, Norway
Phone: +47 38 27 25 20 Fax: +47 38 27 25 49
Org.Nr: NO 980 447 146 MVA

3 Modes of Operation

3.1 Approved Mode of Operation

The validated SecureD cryptographic module always operates in FIPS-mode, and supports FIPS approved algorithms as follows:

- Advanced Encryption Standard (AES) [#1] with 128-, 192-, and 256-bit keys for encryption and decryption in CBC mode (Certificate #383)
- Triple Data Encryption Algorithm (TDEA) [#5], Keying Option 1, 2, 3, for encryption and decryption in CBC mode (Certificate #427)

3.2 Non-FIPS Mode of Operation

The validated SecureD cryptographic module does not support non-FIPS modes of operation.

High Density Devices AS, Postboks 1428, N-4505 Mandal, Norway
Phone: +47 38 27 25 20 Fax: +47 38 27 25 49
Org.Nr: NO 980 447 146 MVA

4 Ports and Interfaces

Table 2 Logical & Physical Interfaces

Logical Interface	Physical Interfaces
Data Input	Host ATA Interface Device ATA Interface ISO 7816
Data Output	Host ATA Interface Device ATA Interface ISO 7816
Status	Status Interface (LED)
Control	Host ATA Interface Device ATA Interface ISO 7816 Utility Interface
Power	5-volt DC input

High Density Devices AS, Postboks 1428, N-4505 Mandal, Norway
Phone: +47 38 27 25 20 Fax: +47 38 27 25 49
Org.Nr: NO 980 447 146 MVA

5 Identification and Authentication Policy

5.1 Assumption of roles

The SecureD cryptographic module supports two distinct operator roles, User and Crypto Officer. The cryptographic module enforces the separation of roles using identity-based operator authentication. The operator of the cryptographic module is uniquely identified by possession of the correct Key Token (smart card) which is uniquely assigned to an individual operator. Possession of the Key Token also determines the role that is assigned to operator possessing the Key Token.

Table 3 Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Data
User	Identity-based operator authentication	TDEA Keys
Crypto Officer	Identity-based operator authentication	TDEA Keys

Table 4 Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
Crypto Officer Key	The probability that a random attempt will succeed or a false acceptance will occur is 2^{-168}, which is less than 1/1,000,000. Authenticating to the module is limited by a timeout period longer than 1 second, resulting in a probability of successfully authenticating to the module within one minute is $< 60*2^{-168}$, which is less than 1/100,000. Maximum number of authentication attempts within one minute is 60.
User Key	The probability that a random attempt will succeed or a false acceptance will occur is 2^{-168}, which is less than 1/1,000,000. Authenticating to the module is limited by a timeout period longer than 1 second, resulting in a probability of successfully authenticating to the module within one minute is $< 60*2^{-168}$, which is less than 1/100,000. Maximum number of authentication attempts within one minute is 60.

High Density Devices AS, Postboks 1428, N-4505 Mandal, Norway
Phone: +47 38 27 25 20 Fax: +47 38 27 25 49
Org.Nr: NO 980 447 146 MVA

6 Access Control Policy

6.1 Roles and Services

Table 5 Services Authorized for Roles

Role	Authorized Services
Crypto Officer	• Crypto Officer Authentication • Set Crypto Officer Key • Set User Key • Set Device Keys • Set Media Resident Keys
User	• User Authentication • Set Media User Keys • Encrypt Data • Decrypt Data • Bypass Data • Erase Media Device Keys

6.1.1 Crypto Officer

This role shall provide all of the services necessary for the Crypto Officer to manage the keying material stored in the SecureD cryptographic module.

6.1.1.1 Crypto Officer Authentication

This service authenticates the Crypto Officer to the SecureD cryptographic module.

6.1.1.2 Set Crypto Officer Key

This service loads the Crypto Officer Key into the SecureD cryptographic module.

6.1.1.3 Set User Key

This service loads the User Key into the SecureD cryptographic module.

6.1.1.4 Set Device Keys

This service loads Device Keys into the SecureD cryptographic module.

6.1.1.5 Set Media Resident Keys

This service loads the Media Resident Keys into the SecureD cryptographic module.

6.1.2 User

This role shall provide all of the services necessary for the encryption and decryption of data passing through the module.

6.1.2.1 User Authentication

This service authenticates the User to the SecureD cryptographic module.

High Density Devices AS, Postboks 1428, N-4505 Mandal, Norway
Phone: +47 38 27 25 20 Fax: +47 38 27 25 49
Org.Nr: NO 980 447 146 MVA

6.1.2.2 Set Media User Keys

This service loads the Media User Keys into the SecureD cryptographic module.

6.1.2.3 Encrypt Data

This service encrypts plaintext user data passed into the cryptographic module.

6.1.2.4 Decrypt Data

This service decrypts encrypted user data passed into the cryptographic module.

6.1.2.5 Bypass Data

This service reads data passed into the cryptographic module without decrypting data. Two independent internal actions activate the capability to prevent the inadvertent bypass of plaintext data due to a single error.

6.1.2.6 Erase Media Device Keys

This service erases all Media Device Keys within the SecureD cryptographic module volatile memory.

6.1.3 Unauthenticated Services

The SecureD cryptographic module supports the following unauthenticated services:

- Show Status: This service provides the current status of the cryptographic module.
- Self Test: This service executes the cryptographic algorithm test for the two security functions (TDEA and AES), using a known answer and firmware integrity tests using a 16-bit EDC.
- Zeroization: This service erases all plaintext Critical Security Parameters (CSPs) that are stored in the SecureD cryptographic module (volatile and non-volatile) memory.
- Reset: This service erases all plaintext Critical Security Parameters (CSPs) that are stored in the SecureD cryptographic module volatile memory.

High Density Devices AS, Postboks 1428, N-4505 Mandal, Norway
Phone: +47 38 27 25 20 Fax: +47 38 27 25 49
Org.Nr: NO 980 447 146 MVA

Table 6 Specification of Service Inputs & Outputs

Service	Control Input	Data Input	Data Output	Status Output
Crypto Officer Authentication	Key Token Interface	Authentication data	N/A	Success/fail
Decrypt Data	Data destination parameters	Encrypted data	Plaintext data	Clear/encrypted
Encrypt Data	Data destination parameters	Plaintext data	Encrypted data	Clear/encrypted
Bypass Data	Data destination parameters	Plaintext data	Plaintext data	Bypass or Alternating
Erase Media Device Keys	Key Token Interface	N/A	N/A	Success/fail
Set Crypto Officer Key	Key Token Interface	TDEA Key	N/A	Success/fail
Set Device Keys	Key Token Interface	TDEA Key	N/A	Success/fail
Set User Keys	Key Token Interface	TDEA Key	N/A	Success/fail
Set Media Resident Keys	Key Token Interface	AES Keys	N/A	Success/fail
Set Media User Keys	N/A	AES Keys	N/A	Success/fail
Show Status	N/A	N/A	N/A	Success/fail
User Authentication	Key Token Interface	Authentication data	N/A	Success/fail
Self Test	Power line Reset line	N/A	N/A	Success/fail
Zeroization	Tamper line	N/A	N/A	Success/fail
Reset	Reset line	N/A	N/A	Success/fail

6.2 Definition of Critical Security Parameters

Table 7 presents the defined Critical Security Parameters (CSPs) and their descriptions.

Table 7 Critical Security Parameter Definitions

CSP	Description/Usage
Media Resident Key	AES 128-, 192-, or 256-bit key for encrypting and decrypting data.
Media User Key	AES 128-, 192-, or 256-bit key for encrypting and decrypting data.
Media Device Key	AES 128-, 192-, or 256-bit key for encrypting and decrypting data.
Crypto Officer Key	TDEA 168-bit key for Crypto Officer authentication.
User Key	TDEA 168-bit key for User authentication.
Device Key 1	TDEA 168-bit key for decrypting cryptographic module data.
Device Key 2	TDEA 168-bit key for decrypting cryptographic module data.

6.3 Definition of Public Keys

There are no public keys contained in the SecureD cryptographic module.

High Density Devices AS, Postboks 1428, N-4505 Mandal, Norway
Phone: +47 38 27 25 20 Fax: +47 38 27 25 49
Org.Nr: NO 980 447 146 MVA

6.4 Definition of CSPs Modes of Access

Table 8 defines the relationship between access to CSPs and the different module services.

Table 8 CSP Access Rights within Roles & Services

Role		Service	Cryptographic Keys and CSP Access Operation
Crypto Officer	User		
X		Crypto Officer Authentication	Crypto Officer Key – read
	X	Decrypt Data	Media Device Keys – read
	X	Encrypt Data	Media Device Keys – read
	X	Erase Media Device Keys	Media Device Keys – write
X		Set Crypto Officer Key	Crypto Officer Key – write
X		Set Device Keys	Device Key 1 – write Device Key 2 - write
X		Set User Key	User Key – write
X		Set Media Resident Keys	Media Resident Keys – write
	X	Set Media User Keys	Media User Keys – write Media Resident Keys – read Media Device Keys – write
	X	User Authentication	User Key – read
N/A	N/A	Show Status	No access
N/A	N/A	Self Test	No access
N/A	N/A	Zeroization	User Key – write Crypto Officer Key – write Device Key 1 – write Device Key 2 – write Media Device Keys – write Media Resident Keys – write
N/A	N/A	Reset	Media Device Keys – write

High Density Devices AS, Postboks 1428, N-4505 Mandal, Norway
Phone: +47 38 27 25 20 Fax: +47 38 27 25 49
Org.Nr: NO 980 447 146 MVA

7 Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements are not applicable because the SecureD cryptographic module does not contain a modifiable operational environment.

High Density Devices AS, Postboks 1428, N-4505 Mandal, Norway
Phone: +47 38 27 25 20 Fax: +47 38 27 25 49
Org.Nr: NO 980 447 146 MVA

8 Security Rules

The SecureD cryptographic module's design corresponds to the SecureD cryptographic module's security rules.

8.1 Security Rules Derived from FIPS 140-2

This section documents the security rules enforced by the cryptographic module to implement the security requirements of this FIPS 140-2 Level 3 module.

a) The cryptographic module provides two distinct operator roles. These are the User role, and the Crypto Officer role.

b) The cryptographic module provides identity-based authentication.

c) When the module has not been placed in a valid role, the operator does not have access to any cryptographic services.

d) The cryptographic module encrypts and decrypts communications with the Key Token using the TDEA algorithm.

e) The cryptographic module encrypts and decrypts data using the AES algorithm.

f) The cryptographic module performs the following tests:

   A. Power up Self Tests:

      1. Cryptographic algorithm tests:

         a. TDEA Known Answer Test

         b. AES Known Answer Test

      2. Firmware Integrity Test (16-bit EDC)

   B. Conditional Self Tests:

      1. Bypass test (Exclusive bypass test and Alternating bypass test)

g) Data output is inhibited during error states and self-tests.

h) Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.

i) The module does not support concurrent operators.

8.2 Security Rules Imposed by the Vendor

This section documents the security rules imposed by the vendor:

1. The Crypto Officer must follow the procedures outlined in the Crypto Officer guidance to properly initialize the cryptographic module from its default manufacturing state and after zeroization.
2. End users must use properly formatted, HDD-approved Key Tokens.
3. The module indicates that it is operating in FIPS mode by the status LED being steady yellow. A steady yellow LED indicates that power up self-tests have completed successfully and that the module is waiting for a Key Token (smartcard) to be inserted. The module always operates in FIPS mode.
4. If the Key Token is removed, SecureD will be set to the timeout policies set by the Key Token, and;
   a) Immediately halt traffic, (indicated to the user by status-LED being steady yellow) or
   b) Timeout after the time specified in the Key Token, (indicated to the user by green blink until the timeout period specified in the Key Token expires, and switching to steady yellow thereafter) or
   c) Continue operation (indicated to the user by green blink) until power off

High Density Devices AS, Postboks 1428, N-4505 Mandal, Norway
Phone: +47 38 27 25 20 Fax: +47 38 27 25 49
Org.Nr: NO 980 447 146 MVA

9 Physical Security Policy

9.1 Physical Security Mechanisms

The SecureD cryptographic module includes the following physical security mechanisms:

- Production-grade materials
- Tamper resistant hard (Shore D 90), opaque material encapsulation of circuitry with removal/penetration attempts causing serious damage
- Tamper label to provide opacity requirements for the chip vendor's own serial number that is visible on the module.

9.2 Operator Required Actions

The operator is required to inspect the SecureD cryptographic module periodically, for evidence of attempts to tamper with the module.

High Density Devices AS, Postboks 1428, N-4505 Mandal, Norway
Phone: +47 38 27 25 20 Fax: +47 38 27 25 49
Org.Nr: NO 980 447 146 MVA

10 Mitigation of Other Attacks Policy

The FIPS 140-2 Area 11 Mitigation of Other Attacks requirements are not applicable because the SecureD cryptographic module does not address attacks outside of the scope of FIPS 140-2.

High Density Devices AS, Postboks 1428, N-4505 Mandal, Norway
Phone: +47 38 27 25 20 Fax: +47 38 27 25 49
Org.Nr: NO 980 447 146 MVA