Protected Item Descriptor

A protected item is defined by the structure in the dongle memory called ***descriptor***. The descriptor contains fields describing the type of data stored in the protected item, its properties, status, activation/deactivation passwords and passwords for executing operations with data.

A protected item/hardware algorithm is addressed by its ***numerical name***. Number name is a 2-byte identifier kept in a special table of item number names and algorithms (Algorithm Root Table, ART). A number name allows identifying the item regardless what memory area is occupies, since the items can be placed randomly in the memory.

Field offset from the beginning of descriptor	Field length (bytes)	Field name	Field description
00h	1	rs_LoFlags	Lower byte of flags, see **nsafl_xxx**
01h	1	rs_algo	Algorithm type, see **rs_algo_XXXX**
02h	2	ReservedForEven	Reserved
04h	4	rs_HiFlags	More flags, see **nsafh_xxx**
08h	4	rs_klen	Data size of protected item or dongle (determinant) algorithm in bytes **(rs_K[])**
0C	4	rs_blen	Size of data block for hardware algorithm
10	8	rs_hash	This field is reserved and must be filled with 0
18	4	rs_ActivatePwd	Activation password (if flag **nsafl_ActivationSrv** exists)
1C	4	rs_DeactivatePwd	Deactivation password (if flag **nsafl_DeactivationSrv** exists)
20	4	rs_ReadPwd	Password for reading fields **rs_GP, rs_ErrorCounter, rs_K[]** using **GrdPI_Read** function (if flag **nsafh_ReadPwd** exists)
24	4	rs_UpdatePwd	Password for updating field **rs_GP, rs_ErrorCounter, rs_K[]** using **GrdPI_Update** function(if flag **nsafh_UpdateSrv** exists)
28	6	rs_BirthTime	
2E	6	rs_DeadTime	
34	8	rs_Lifetime	
3C	8	rs_FlipTime	
44	4	rs_GP	Reverse counter
48	4	rs_ErrorCounter	Permissible number of password entry attempts (if one of the following flags exists: nsafl_ **ActivationSrv, nsafl_DeactivationSrv** or **nsafl_UpdateSrv)**
4C	rs_klen	rs_K[]	Protected item data or algorithm determinant sized **rs_klen**

Field **rs_LoFlags** contains lower byte of flags defining the properties of protected items. The following flags can be set (flag names listed below are used in Guardant API):

Flag name	Value	Comment
nsafl_ID	1	
nsafl_GP_dec	2	Decrements GP counter on each algorithm call. Once GP counter reaches 0, algorithm is automatically deactivated and returns error code **GrdE_InactiveItem** in response to further calls
nsafl_GP	4	Not used for modern dongles
nsafl_ST_III	8	Flag should be set for modern dongles
nsafl_ActivationSrv	16	Activation service available

nsafl_DeactivationSrv	32	Deactivation service available
nsafl_UpdateSrv	64	Password-protected service for changing data in items **rs_K[]** available **(GrdPI_Update** function supported)
nsafl_InactiveFlag	128	Algorithm/cell is inactive at the moment. Operations **GrdTransform, GrdPI_Read, GrdPI_Update** not available

Flag name / Algorythm type	AES128,GSII64	ECC160	SHA256	Loadable Code	Protected Item
nsafl_ID	+	-	-	-	-
nsafl_GP_dec	+	+	+	+	-
nsafl_GP	-	-	-	-	-
nsafl_ST_III	+	+	+	+	-
nsafl_ActivationSrv	+	+	+	+	+
nsafl_DeactivationSrv	+	+	+	+	+
nsafl_UpdateSrv	+	+	+	+	+
nsafl_InactiveFlag	+	+	+	+	+
nsafh_ReadSrv	+	+	+	+	+
nsafh_ReadPwd	+	+	+	+	+
nsafh_BirthTime	+	+	+	+	-
nsafh_DeadTime	+	+	+	+	-
nsafh_LifeTime	+	+	+	+	-
nsafh_FlipTime	+	-	-	-	-

Field **rs_algo** contains protected item type code.

a. The following protected item type codes available for Guardant Sign/Time/Net dongles:

Flag name	Value	Comment
	0-4	Reserved
rs_algo_GSII64	5	Symmetrical data encryption algorithm. 128 or 256-bit secret key
rs_algo_HASH64	6	Calculation of 64-bit hash. 128 or 256-bit secret key
rs_algo_RND64	7	Generation of 64-bit random number
rs_algo_PI	8	Protected item
rs_algo_GSII64_ENCRYPT	10	
rs_algo_GSII64_DECRYPT	11	
rs_algo_ECC160	12	
rs_algo_AES128	13	
rs_algo_SHA256	15	

b. The following protected item type codes available for Guardant Code/Code Time:

Flag name	Value	Comment
rs_algo_PI	8	Protected item
rs_algo_ECC160	12	

rs_algo_AES128	13	
rs_algo_LoadableCode	14	
rs_algo_SHA256	15	
rs_algo_AES128Encode	16	
rs_algo_AES128Decode	17	

Field **rs_HiFlags** contains 4 bytes of flags defining the properties of protected items. The following flags can be set (flag names listed below are used in Guardant API):

Flag name	Value	Comment
nsafh_ReadSrv	1	Service of reading data in items **rs_K[]** available **(GrdPI_Read** function supported)
nsafh_ReadPwd	2	Reading is password-protected **(rs_ReadPwd)**
nsafh_BirthTime	4	
nsafh_DeadTime	8	
nsafh_LifeTime	16	
nsafh_FlipTime	32	

Field **rs_klen** contains the size of data **rs_K[]** stored in the protected item (dongle secret key) in bytes.

Field **rs_blen** contains data block size for hardware algorithm. Possible values :

Algorythm Type	Private key length (rs_klen), B	Minimum data block size (rs_blen), B
GSII64	GrdADS_GSII64=16/32	GrdARS_GSII64=8
HASH64	GrdADS_HASH64=16/32	GrdARS_HASH64=8
RND64	GrdADS_RAND64=16/32	GrdARS_RAND64=8
AES128	GrdADS_AES128=16	GrdARS_AES128=16
ECC160	GrdADS_ECC160=20	GrdARS_ECC160=20
SHA256	-	GrdARS_HASH_SHA256=0
Loadable Code	sizeof(TGrdLoadableCodeData)	N/A

If a wrong value is entered for GSII64, HASH64 and RND64 hardware algorithms, the private key size is set to 16 bytes by default.

Field **rs_hash** is reserved for future use.

Field **rs_ActivatePwd** contains 4-byte protected item activation password if activation service is enabled by setting flag **nsafl_ActivationSrv.**

Field **rs_DeactivatePwd** contains 4-byte protected item deactivation password if deactivation service is enabled by setting flag **nsafl_DeactivationSrv.**

Field **rs_ReadPwd** contains 4-byte protected item reading password if data reading service is enabled by setting flag **nsafh_ReadPwd.**

Field **rs_UpdatePwd** contains 4-byte protected item update password if data update service is enabled by setting flag **nsafh_UpdateSrv.**

Offset	Size	Name	Value
0	BYTE	BSeconds	0 <= Seconds <= 59
1	BYTE	BMinute	0 <= Minutes <= 59
2	BYTE	BHour	0 <= Hours <= 23

3	BYTE	BDay	1 <= Days <= 31
4	BYTE	BMonth	1 <= Months <= 12
5	BYTE	BYear	0 <= Years <= 99, since 2000

Field **rs_GP** contains an algorithm counter. If flag **nsaf_GP_dec** is set, this field defines the number of times the algorithm will be executed. Upon reaching zero the algorithm will be deactivated & will stop converting the data. **GrdE_InactiveItem** error code will return upon further calls. This field can be increased only by completely rewriting the descriptor.

Field **rs_GP** contains an algorithm counter. If flag **nsaf_GP_dec** is set, this field defines the number of times the algorithm will be executed. Upon reaching zero the algorithm will be deactivated & will stop converting the data. **GrdE_InactiveItem** error code will return upon further calls. This field can be increased only by completely rewriting the descriptor.

Field **rs_K[]** contains protected item data. Depending on the item type it may be used for storing the secret algorithm key, LMS license table or any other data. The size of data should match the value of **km_ad_klen** field. The data in the protected items can be accessed or edited only using special functions. The main difference of a protected item from simple data is that the data stored in the protected item can be changed only using a special password. Such mechanism provides for safer alteration of a part of dongle memory without affecting the rest of the memory.