NOTITIE: ST 19-19

Aan	:	College van Deskundigen voor Veilige en Inbraakwerende producten (CvD-V&I)
Onderwerp	:	Voorstel toevoeging eisen Biometrische bediening
Van	:	Charles Wallert
Datum	:	19-11-2019

Geachte leden van het College,

In AE 3104 par 02 zijn aanvullende product eisen – elektro – mechanische H&S opgenomen.
V.w.b. biometrische bedieningen waren nog geen eisen opgenomen.
In ST 19-15 AE 3104 pag. 7 is onderstaand voorstel opgenomen;

Biometrische bediening
_ Valse herkenningsgraad - False Recognition Rate (FAR): < 0,001%
_ Valse afwijzingsgraad - False Rejection Rate (FRR): < 1%

Bij nader inzien, gezien publicatie van NEN 5089 (ST 19-14), waarbij “mechatronisch deurbeslag” voor biometrische bediening wordt verwezen naar digit 7: grade B & C van prEN 16867 is het voorstel om voor overige elektromechanische bedieningen gelijke eisen te stellen, zie onderstaand (gele markering)

4.7 Credential related security (7th character)

4.7.1 General

The MDF and its credentials for grade A to D shall have security against code manipulations, brute force attacks, credential copying, code spying and code guessing regardless of the technique used.

The requirements for the credential related security vary with the different credential techniques used for the MDF. Table 5 shows the requirements for RFID (radio frequency identification, active or passive), PIN code, magnetic stripe and biometric techniques.

If the method of obtaining access to the MDF does not fall into any of these categories, the credential related security grade shall be declared by analogy to the best comparable technique.

In the case where the MDF may be authorized by two of the techniques the grade for credential related security depends on whether both techniques may be used alternatively to gain access or both techniques are always used together to gain access. In the first case, the grade is the lower one of the grades of the individual techniques, in the latter case the grade is one grade higher than the highest grade of the individual technique, but not higher than the highest possible grade D.

Verified according to 6.7.

Table 5 — Credential related security

Technique	Requirements	0	A	B	C	D
ICC	code variations / max number of auth. codes	NPD	10 000	1 000 000	1 000 000	10 000 000
	encryption	NPD	no requirement.	no requirement.	yes	communication encrypted with AES or 3DES; session keys, unique key
	encryption key length	NPD	no requirement.	no requirement.	48 bits	128 bits AES 3x56 bits 3DES
	copy protection	NPD	no requirement.	no requirement.	yes	yes

®copyright SKG

Technique	Requirements	0	A	B	C	D
PIN code	code variations / max number of auth. codes	NPD	1 000	10 000	-	-
	Additional security features	NPD	dead time after failed attempt	dead time after failed attempt and protected visibility	-	-
	T = the maximum number of codes of the unit divided by the read speed (the number of possible codes per hour), divided by the number of possible users and divided by 2.	NPD	T = 6 h	T = 24 h	-	-
Access Card	code variations / max number of auth. codes	NPD	10 000	1 000 000	-	-
	copy protection	NPD	no requirement	no requirement	-	-
	T = the maximum number of codes of the unit divided by the read speed (the number of possible codes per hour), divided by the number of possible users and divided by 2.	NPD	T = 6 h	T = 24 h	-	-
Biometrics	FAR^{-1} / max. number of auth. templates	NPD	100	1 000	10 000	-
	Additional security features	NPD	no requirement	alive detection	alive detection	-

NOTE Grade D is not achievable for pure PIN code, access card or biometric systems.

4.7.2 ICC

4.7.2.1 Effective code variations

The effective code variations are all code variations possible by design divided by the maximum possible number of authorized codes on one MDF. It shall be at least the number according to Table 5.

NOTE: In the case where the unique ID of the RFID is used, this corresponds to the possible variations of the unique ID divided by the maximum possible number of authorized credentials.

NOTE Examples are given in Annex E.

4.7.2.2 Encryption

In grade C, the data on the RFID or the communication between RFID and MDF shall be encrypted by any encryption algorithm. The length of the encryption key shall be at least 48 bits long.

®copyright SKG

In grade D, the communication between the RFID and the MDF shall be encrypted by the AES or 3DES (TDEA) encryption method according to ISO/IEC 18033-3:2010.

The encryption key shall be at least 128 bits long. For each communication attempt (session) a new session key shall be created and used for the communication. Session keys and encryption keys shall never be broadcasted (challenge response technique). The encryption key shall be unique for each system installation of MDFs or, alternatively, shall be user configurable.

4.7.2.3 Copy protection

In grades C and D the credential shall be copy protected. It shall not be possible to copy an authorized credential using standard third party equipment.

4.7.3 PIN Code

4.7.3.1 Effective code variations

The effective code variations are the possible code variations divided by the maximum number of possible authorized codes on one MDF. It shall be at least the number according to Table 5.

NOTE In the case of a 4 digit PIN code and a maximum number of 10 users, the effective code variations are 1 000.

4.7.3.2 Dead time failed attempts

The MDF shall have the security feature that makes it impossible to try out all or a large portion of all possible codes within a reasonable time.

4.7.3.3 Protected visibility

For MDFs grade B the included angle over which any code information may optically be observed shall be not more than 30° about the vertical centre-line.

4.7.3.4 Mean time to gain access by trying

The mean time to gain access by trying T shall be greater than the time stated in Table 5. T is calculated by the maximum number of codes of the unit divided by the read speed (the number of possible codes per hour), divided by the number of possible users, divided by 2.

4.7.4 Access Card

4.7.4.1 Effective code variations

The effective code variations are all code variations possible by design divided by the maximum possible number of authorized codes on one MDF. It shall be at least the number according to Table 5.

4.7.4.2 Mean time to gain access by trying

The mean time to gain access by trying T shall be greater than the time stated in Table 5. T is calculated by the maximum number of codes of the unit divided by the read speed (the number of possible codes per hour), divided by the number of possible users, divided by 2.

4.7.5 Biometrics

4.7.5.1 FAR−1 divided by maximum number of authorized templates

The analogy of effective code variations in biometric systems is the inverse of the false acceptance rate (FAR-1) divided by the maximum possible number of authorized templates on one MDF. It shall be at least the number according to Table 5.

FprEN 16867:2019 (E)

4.7.5.2 Alive detection

In grades B and C the MDF shall be able to detect whether the presented credential (fingerprint, hand vein image, iris image) comes from an alive human to prevent that artificially produced images may be successfully presented to the MDF.

®copyright SKG