Melléklet a 001/2005. számú kijelölési okirathoz

Kijelölt szervezet: **MATRIX Vizsgáló, Ellenőrző és Tanúsító Kft.**
2040, Budaörs, Szabadság út 290.

Tevékenység jellege: **az elektronikus aláírási termékek tanúsítása**

A tevékenységre vonatkozó mértékadó előírások:

2001. évi XXXV. törvény az elektronikus aláírásról
151/2001. (IX. 1.) Korm. rendelet a Hírközlési Főfelügyeletnek az elektronikus aláírással kapcsolatos feladat- és hatásköréről, valamint eljárásának részletes szabályairól
16/2001. (IX. 1.) MeHVM rendelet az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről
15/2001. (VIII. 27.) MeHVM rendelet az elektronikus aláírási termékek tanúsítását végző szervezetekről, illetve a kijelölésükre vonatkozó szabályokról
2/2002. (IV. 26.) MeHVM irányelv a minősített elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó biztonsági követelményekről

TTKK-45011-2 Terméktanúsítási Minőségügyi Kézikönyv az elektronikus aláírási termékek megfelelőségének tanúsítására
MSZ EN 45011 terméktanúsítási irányító tanúsítási szervezetekre vonatkozó általános feltételek
MSZ EN ISO 9001 minőségirányítási rendszer követelmények

Az elektronikus aláírási termékek megfelelőségének tanúsítására vonatkozó szabványok és ajánlások.

SZABVÁNY / AJÁNLÁS JELÖLÉSE	SZABVÁNY / AJÁNLÁS CÍME / TARTALMA
CEN CWA 14167-1	Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures/ Biztonsági követelmények elektronikus aláírások tanúsítványainak kezelését végző megbízható rendszerek számára July 17, 2001
CEN HSM-PP	/Hardware Security Module Protection Profile/ Hardver biztonsági modul védelmi profil /draft / 21 June, 2001

SZABVÁNY / AJÁNLÁS JELÖLÉSE	SZABVÁNY / AJÁNLÁS CÍME / TARTALMA
Dobbertin, H., A. Bosselaers, and B. Preneel, "RIPEMD-160:	A strengthened version of RIPEMD," In Fast software encryption, Proc. third International Workshop, Cambridge, UK, February 21-23, 1996, pp. 71-82, D. Gollmann (ed.), LNCS 1039, Springer-Verlag, 1996
FIPS 140-1 / 140-2	Security Requirements for Cryptographic Modules, Federal Information Processing Standards Publication 140-1, January 11, 1994 / May25, 2001
ISO/IEC 10118 - 1:	Hash functions, Part 1.: General model
ISO/IEC 10118 - 2:	Hash functions, Part 2.: n-bit block cipher
ISO/IEC 10118 -3:	Information technology - Security techniques - Hash functions - Part 3: Dedicated Hash Functions, 1998
ISO/IEC 10118 - 4:	Hash functions, Part 4.: Modular arithmetic
ISO/IEC 14888 – 1	Digital signature: General model
ISO/IEC 14888 – 2	Digital signature: Identity based (GQ)
ISO/IEC 14888 - 3:	Information technology - Security techniques - Digital signatures with appendix – Part 3: Certificate-based mechanisms, 1999
ISO/IEC 15946	Cryptographic techniques based on elliptic curves, 1999, 2000
ISO/IEC 18031	Random number generation 2000
ISO/IEC 1999:15408	Információ technológia - Biztonsági módszerek - Informatikai biztonság értékelési kritériumai (1-3) része
ISO/IEC DIS 17799:	„Információ biztonsági eljárási kódex".
ITSEC:	Information Technology Security Evaluation Criteria
BS 7799	Information security management
NIST: FIPS 180-1 Publication	Secure Hash Standard (SHS-1), 1995.

SZABVÁNY / AJÁNLÁS JELÖLÉSE	SZABVÁNY / AJÁNLÁS CÍME / TARTALMA
NIST: FIPS 186-2 Publication	Digital Signature Standard (DSS), January 2000.
Rivest, R., A. Shamir, and L. Adleman,	"A method for obtaining digital signatures and public key cryptosystems," Communications of the ACM, Vol. 21, No. 2, 1978, pp. 120-126
RSA Laboratories, PKCS #1 v2.0:	RSA Cryptography Standard," October 1998
RSA Laboratories, "PKCS #1 v2.1 2:	RSA Cryptography Standard," January 2001.
ISO / IEC 9798 - 1	Entity Authentication Part 1. General model
ISO / IEC 9798 - 2	Entity Authentication Part 2.: Symmetric encipherment algorithms
ISO / IEC 9798 - 3	Entity Authentication Part 3.: Symmetric techniques
ISO / IEC 9798 - 4	Entity Authentication Part 4.: Cryptographic check functions
ISO / IEC 9798 - 5	Entity Authentication Part 5.: ZKN techniques.
ISO / IEC 13888 – 1	Non repudiation, Part 1.: General model
ISO / IEC 13888 – 2	Non repudiation, Part 2.: Symmetric techniques
ISO / IEC 13888 - 3	Non repudiation, Part 3.: Asymmetric techniques
ISO / IEC 9796 – 1	Digital signature giving message recovery: redundancy
ISO / IEC 9796 – 2	Digital signature schemes giving message recovery: hash-functions, ISO/IEC DIS
ISO / IEC 9796 – 3	Mechanisms using check functions
ISO / IEC 9796 – 4	Discrete logarithm based mechanisms
ISO / IEC 9979	Directory of cryptographic algorithms
ISO / IEC 9372	Modes of operation for 64 bit block cipher algorithms
ISO / IEC 10116	Modes of operation for n-bit block cipher algorithms

SZABVÁNY / AJÁNLÁS JELÖLÉSE	SZABVÁNY / AJÁNLÁS CÍME / TARTALMA
ISO / IEC 13335 – 1	Guidelines for the management of IT Security: Concepts and models.
ISO / IEC 13335 – 2	Guidelines for the management of IT Security: Managing and planning.
ISO / IEC 13335 – 3	Guidelines for the management of IT Security: Techniques for the management
ISO / IEC 13335 – 4	Guidelines for the management of IT Security: Selection of safeguards
ISO / IEC 13335 - 5	Guidelines for the management of IT Security: External connections
ISO / IEC 11770 – 1	Key management, Part 1.: Framework
ISO / IEC 11770 – 2	Key management, Part 2.: Symmetric techniques
ISO / IEC 11770 - 3	Key management, Part 3.: Asymmetric techniques
ISO / IEC 14516 – 1	TTP (Trusted Third Party) General overview
ISO / IEC 14516 - 2	Guidelines for the use and management of TTP (Trusted Third Party) Technical aspects
ISO / IEC 11568 - 3	Banking – key management techniques for symmetric ciphers
ISO / IEC 9594 – 8 X. 509v3	Certificate extensions and CRL extensions
ISO / IEC 7810	Identification cards – Physical Characteristics, ISO IS1995
ISO / IEC 7813	ISO Identification cards – Financial transaction cards, Physical characteristics, ISO IS 1995
ISO / IEC 7816 – 1	Identification cards – Integrated circuit(s) cards with contacts; Part 1.: Physical characteristics, ISO IS 1995
ISO / IEC 7816 – 2	Identification cards – Integrated circuit(s) cards with contacts; Part 2.: Dimension and location of contacts
ISO / IEC 7816 – 3	Identification cards – Integrated circuit(s) cards with contacts; Part 3.: Electronic signals and transmission protocols

SZABVÁNY / AJÁNLÁS JELÖLÉSE	SZABVÁNY / AJÁNLÁS CÍME / TARTALMA
ISO / IEC 7816 – 4	Identification cards – Integrated circuit(s) cards with contacts; Part 4.: Interindustry commands for interchange
ISO / IEC 7816 – 5	Identification cards – Integrated circuit(s) cards with contacts; Part 5.: Numbering system and registration procedure application indicators
ISO / IEC 7816 – 6	Identification cards – Integrated circuit(s) cards with contacts; Part 6.: Interindustry data elements
ISO / IEC 7816 - 7	Identification cards – Integrated circuit(s) cards with contacts; Part 6.: Interindustry commands for structured card query language (SCQL)
ISO / IEC 7816 - 8	Identification cards – Integrated circuit(s) cards with contacts; Part 8.: Security related industry commands
ISO / IEC 10373	Identification cards – Test methods ISO / IEC IS 1993
RFC 1320	The MD4 message-digest algorithm, R. Rivest, Internet Activities Board, internet Privacy Task Force, April 1992
RFC 1421	Message encryption and authentication Procedures
RFC 1422	Kent, S., "Privacy Enhancement for Internet Electronic Mail: Part II: Certificate based key management, BBN, February 1993
RFC 1423	Algorithms, Models and Indicators
RFC 1424	Key certification and related services
PKCS #1 - #11	Public key cryptography Standards
CEN ENV 1375 - 1	Identification card system – Intersector integrated circuit(s) card additional formats – part 1.: ID-000 card size and physical characteristics
DIN EN 45001	General criteria for operation of test laboratories Allgemeine Kriterien zum Betreiben von Prüflaboratorien (September 1989)
DIN EN 45004	General criteria for operation of different types of bodies which carry out inspections Allgemeine Kriterien den Betrieb verschiedener Typen von Stellen, die Inspektionen durchführen (Juni 1995)

SZABVÁNY / AJÁNLÁS JELÖLÉSE	SZABVÁNY / AJÁNLÁS CÍME / TARTALMA
DIN EN 45011	General criteria for bodies which certify products; Allgemeine Kriterien für Stellen, die Produkte zertifizieren. (May 1990)
X.509	ITU-T Recommendation X.509, Information Technology – Open Systems Interconnection – The directory: authentication framework
X.509v3	ITU-T Recommendation X.509, Information Technology – Open Systems Interconnection – The directory: authentication framework, amendment 1: Certificate Extension, Final Draft 1996
PKIX	Internet Public Key Infrastructure, Internet drafts: Web based Certificate and CRL Repository; Part 1.: X.509 Certificate and CRL Profile Part 2: Operational protocols Part 3.: Certificate Management Protocols Part 4.: Certificate Policy and Certification Practices Framework
NIST - FIPS 197	AES: Advanced Encryption Standard, The RIJDAEL Block Cipher
ANSI X.9.30. - 1	Public Key cryptography using irreversible algorithms for the financial services industries: Part 1.: The Digital Signature Algorithm (DSA), 1993
ANSI X.9.30. - 2	Public Key cryptography using irreversible algorithms for the financial services industries. Part 2.: The Secure Hash algorithm (SHA-1), 1993
IEEE 1363	Standard for RSA, Diffie-Hellman and related Public-Key Cryptography, 1998

A fenti lista folyamatos aktualizálását a tanúsítónak kell elvégezni.