

# Tartalomjegyzék

<b>AZ ELEKTRONIKUS ALÁÍRÁS JOGI ÉS TECHNOLÓGIAI KÖRNYEZETE AZ EURÓPAI UNIÓBAN ÉS MAGYARORSZÁGON</b> .....	<b>1</b>
<b>TARTALOMJEGYZÉK</b> .....	<b>2</b>
<b>AZ ALÁÍRÁSOK TECHNIKAI ÉS JOGI KILÁTÁSAI</b> .....	<b>5</b>
<b>AZ ALÁÍRÁSOK TECHNIKAI ÉS JOGI KILÁTÁSAI</b> .....	<b>5</b>
A BIZTONSÁGI SZOLGÁLTATÁSOK TECHNIKAI DEFINÍCIÓI .....	5
TECHNIKAI ÉS JOGI SZEMPONTOK.....	6
ALÁÍRÁSOK FUNKCIONÁLIS NÉZŐPONTBÓL.....	7
A NEM TECHNOLÓGIAI BIZONYÍTÉK SZÜKSÉGESSÉGE.....	9
AZ ALÁÍRÁSI DEFINÍCIÓK ÖSSZEHASONLÍTÁSA.....	10
<i>A digitális aláírás definíciója</i> .....	10
<i>Az elektronikus aláírás definíciója</i> .....	11
<b>AZ ELEKTRONIKUS ALÁÍRÁS HELYZETE AZ EURÓPAI UNIÓBAN</b> .....	<b>12</b>
<b>AZ ELEKTRONIKUS ALÁÍRÁS MAGYARORSZÁGON</b> .....	<b>17</b>
TÖRVÉNYI HÁTTÉR.....	17
AZ ELEKTRONIKUS ALÁÍRÁS HAZAI HASZNÁLATA.....	18
<i>A magánszemélyek és az elektronikus aláírás</i> .....	19
<i>Az elektronikus aláírás használata vállalatoknál</i> .....	21
<i>A hazai hitelesítés-szolgáltatók</i> .....	23
<i>Az elektronikus aláíráshoz szükséges eszközök gyártói</i> .....	24
<b>AZ ELEKTRONIKUS ALÁÍRÁSSAL KAPCSOLATOS SZABVÁNYOK</b> .....	<b>25</b>
BEVEZETÉS .....	25
A CSOPORTOKBA SOROLT SZABVÁNYOK LISTÁJA.....	26
A NYILVÁNOS KULCSÚ INFRASTRUKTÚRÁHOZ KAPCSOLÓDÓ EGYÉB SZABVÁNYOK .....	42
<b>SZÓSZEDET</b> .....	<b>53</b>
<b>IRODALOMJEGYZÉK</b> .....	<b>54</b>
<b>ELEKTRONIKUS ALÁÍRÁS SZABÁLYZAT</b> .....	<b>55</b>
<b>BEVEZETÉS</b> .....	<b>56</b>
<b>ELEKTRONIKUS ALÁÍRÁSI SZABÁLYZAT</b> .....	<b>58</b>
<b>FOGALMAK, ÁLTALÁNOS RENDELKEZÉSEK</b> .....	<b>58</b>
<b>A KIADMÁNYOZÁS RENDJE</b> .....	<b>60</b>
<b>ÜGYIRATKEZELÉS</b> .....	<b>61</b>
<b>AZ ELEKTRONIKUS ALÁÍRÁS SZABÁLYAI</b> .....	<b>62</b>
<b>AZ ARCHIVÁLÁS SZABÁLYAI</b> .....	<b>68</b>
<b>AZ ELEKTRONIKUS ALÁÍRÁS FELHASZNÁLÁSA A SZERVEZETBEN</b> .....	<b>70</b>
<b>MODELL ÉS MÓDSZERTAN AZ ELEKTRONIKUS ALÁÍRÁS-LÉTREHOZÓ ÉS ELLENŐRZŐ ALKALMAZÁSOK VIZSGÁLATÁRA</b> .....	<b>72</b>
<b>BEVEZETÉS</b> .....	<b>73</b>
<b>ÉRVÉNYESSÉGI KÖR</b> .....	<b>73</b>
<b>AZ ALÁÍRÁS-LÉTREHOZÁS FUNKCIONÁLIS MODELLJE</b> .....	<b>74</b>
ALÁÍRÁS-LÉTREHOZÓ ALKALMAZÁS.....	78
<b>AZ ALÁÍRÁS-ELLENŐRZŐ RENDSZEREK FUNKCIONÁLIS MODELLJE</b> .....	<b>80</b>
AZ ALÁÍRÁS ÉLETTARTAMA .....	80

A KEZDETI- ÉS AZ UTÓLAGOS ELLENŐRZÉSI FOLYAMAT .....	81
A KEZDETI ELLENŐRZÉSI FOLYAMAT ALAPVETŐ BEMENŐ ADATAI.....	81
A KEZDETI ALÁÍRÁS-ELLENŐRZÉSI FOLYAMAT KIMENŐ ÉRTÉKEI.....	82
A KEZDETI ELLENŐRZŐ RENDSZER.....	83
<b>KÖVETELMÉNYEK AZ ALÁÍRÁS-LÉTREHOZÓ ALKALMAZÁS (SCA) EGÉSZÉRE.....</b>	<b>84</b>
AZ ALÁÍRÁS-LÉTREHOZÓ ALKALMAZÁS ÉS A BIZTONSÁGOS ALÁÍRÁS-LÉTREHOZÓ ESZKÖZ KÖZÖTTI MEGBÍZHATÓ ÚTVONALRA VONATKOZÓ KÖVETELMÉNYEK .....	84
<i>A megbízható útvonal alapkövetelményei.....</i>	84
<i>A nyilvános aláírás-létrehozó alkalmazásokra vonatkozó követelmények.....</i>	85
<i>A pontos hivatkozás az aláíró dokumentumára és az aláíró tulajdonságaira .....</i>	85
OSZTOTT ARCHITEKTÚRÁJÚ ALÁÍRÁS-LÉTREHOZÓ ALKALMAZÁSOKRA VONATKOZÓ KÖVETELMÉNYEK .....	86
<i>Osztott architektúrájú aláírás-létrehozó alkalmazások konfigurációira vonatkozó követelmények.....</i>	86
A NEM MEGBÍZHATÓ FOLYAMATOKBÓL ÉS KOMMUNIKÁCIÓS PORTOKBÓL ADÓDÓ KÖVETELMÉNY .....	86
<i>A nem megbízható aláírás-létrehozó alkalmazás-összetevők ellen való védekezésre vonatkozó követelmények.....</i>	86
AZ ALÁÍRANDÓ ADATRA VONATKOZÓ KÖVETELMÉNYEK .....	86
<i>Az aláírandó adat összetevőire vonatkozó követelmények.....</i>	86
KÖVETELMÉNYEK AZ ALÁÍRÓ DOKUMENTUMÁT MEGJELENÍTŐ ÖSSZETEVŐRE (SDP).....	87
<i>A tartalomformátumra vonatkozó követelmények.....</i>	87
<i>Az aláíró dokumentumára vonatkozó egyértelműségi követelmény.....</i>	89
<i>A nem megjelenítés-érzékeny aláírói dokumentumokra vonatkozó követelmény.....</i>	89
<i>A rejtett szövegre és aktív kódra vonatkozó követelmény .....</i>	89
KÖVETELMÉNYEK AZ ALÁÍRÁS TULAJDONSÁGOKAT MEGJELENÍTŐ ÖSSZETEVŐRE (SAV) .....	90
<i>Az aláírás tulajdonságot megjelenítőre vonatkozó biztonsági követelmények.....</i>	90
A TANÚSÍTVÁNYOK MEGJELENÍTÉSÉRE VONATKOZÓ BIZTONSÁGI KÖVETELMÉNYEK .....	91
<i>A tanúsítványok megjelenítésére vonatkozó biztonsági követelmények .....</i>	91
KÖVETELMÉNYEK AZ ALÁÍRÓVAL KÖLCSÖNHATÓ ÖSSZETEVŐRE (SIC) .....	92
<i>Az aláírás kiváltására vonatkozó követelmények.....</i>	92
<i>Az inaktivitási időkorlátra vonatkozó biztonsági követelmények.....</i>	92
<i>A felhasználói interfész megjelenése .....</i>	92
KÖVETELMÉNYEK AZ ALÁÍRÓT HITELESÍTŐ ÖSSZETEVŐRE (SAC) .....	93
<i>A tudáson alapuló aláíróit hitelesítő adatokra vonatkozó biztonsági követelmények.....</i>	93
<i>A biometrikus, aláíróit hitelesítő adatokra vonatkozó biztonsági követelmények.....</i>	94
KÖVETELMÉNYEK AZ ALÁÍRANDÓ ADAT FORMÁZÓ ÖSSZETEVŐRE (DTBSF) .....	95
<i>Az aláírandó adat formázó összetevőre vonatkozó biztonsági követelmények .....</i>	95
KÖVETELMÉNYEK AZ ADAT LENYOMAT KÉSZÍTŐ ÖSSZETEVŐRE (DHC).....	96
<i>Az adat lenyomat készítő összetevőre vonatkozó biztonsági követelmények.....</i>	96
KÖVETELMÉNYEK A BIZTONSÁGOS ALÁÍRÁS-LÉTREHOZÓ ESZKÖZ ÉS AZ ALÁÍRÁS-LÉTREHOZÓ ALKALMAZÁS (SSCD/SCA) KÖZÖTTI KOMMUNIKÁCIÓ ÖSSZETEVŐRE (SSC) .....	96
<i>A biztonságos aláírás-létrehozó eszköz és az aláírás-létrehozó alkalmazás közötti kommunikáció összetevőre vonatkozó biztonsági követelmények.....</i>	96
KÖVETELMÉNYEK A BIZTONSÁGOS ALÁÍRÁS-LÉTREHOZÓ ESZKÖZ ÉS AZ ALÁÍRÁS-LÉTREHOZÓ ALKALMAZÁS (SSCD/SCA) HITELESÍTŐ ÖSSZETEVŐRE (SSA).....	97
<i>A biztonságos aláírás-létrehozó eszköz és az aláírás-létrehozó alkalmazás-hitelesítő összetevőre vonatkozó biztonsági követelmények .....</i>	97
KÖVETELMÉNYEK AZ ALÁÍRANDÓ DOKUMENTUM ELŐKÉSZÍTŐ ÖSSZETEVŐRE .....	98
<i>Az aláírandó dokumentum előkészítő összetevőre vonatkozó biztonsági követelmények.....</i>	98
KÖVETELMÉNYEK AZ INPUT/OUTPUT INTERFÉSZRE (I/O).....	98
<i>Az Input vezérlésre vonatkozó biztonsági követelmények.....</i>	98
<b>KÖVETELMÉNYEK AZ ALÁÍRÁS-ELLENŐRZŐ RENDSZER (SVS) EGÉSZÉRE .....</b>	<b>99</b>
AZ ALÁÍRÁS ELLENŐRZÉSI RENDSZER FOLYAMATAIRA VONATKOZÓ KÖVETELMÉNYEK .....	99
<i>Azonnali és utólagos ellenőrzés.....</i>	99
<i>Az ellenőrzéshez szükséges adatokkal szemben támasztott követelmények.....</i>	99
<i>Aláírási formátumok az ETSI TS 101 733 és az ETSI TS 101 903 szabvány szerint.....</i>	99
<i>Azonnali ellenőrzés bemeneti adatai .....</i>	100
<i>Azonnali ellenőrzés kimeneti adatai.....</i>	100
<i>Az ellenőrzéshez begyűjtött adatok .....</i>	100
<i>Az ellenőrzéshez begyűjtött adatok kiterjesztése.....</i>	100
<i>Az ellenőrzési folyamat szabályai.....</i>	101

Minősített tanúsítvánnyal létrehozott elektronikus aláírás ellenőrzése .....	101
Minősített elektronikus aláírás ellenőrzése .....	101
A visszavonási adatok feldolgozásának szabályai .....	102
A tanúsítási láncolat .....	102
A kriptográfiai algoritmusok és kulcsok szabályai .....	102
<b>ALÁÍRÁS-ELLENŐRZŐ RENDSZEREK .....</b>	<b>103</b>
<i>Kézi ellenőrzés</i> .....	<i>103</i>
Az aláírt dokumentum megjelenítése .....	103
Az aláíró tulajdonságainak és az ellenőrzés kimenetének megjelenítése .....	103
A felhasználói felülettel szemben támasztott követelmények .....	103
<b>ALÁÍRÁS-ELLENŐRZŐ RENDSZEREK BIZTONSÁGI KÖVETELMÉNYEI .....</b>	<b>104</b>
<i>A biztonságos eszközökkel szemben támasztott követelmények</i> .....	<i>104</i>
<i>Az ellenőrzési folyamat</i> .....	<i>104</i>
<b>SZÓSZEDET .....</b>	<b>105</b>
<b>IRODALOMJEGYZÉK .....</b>	<b>106</b>
<b>MEGFELELŐSÉG-VIZSGÁLAT AZ ELEKTRONIKUS ALÁÍRÁS-LÉTREHOZÓ ÉS ELLENŐRZŐ ALKALMAZÁSOK VIZSGÁLATÁRÓL SZÓLÓ MÓDSZERTANHOZ .....</b>	<b>107</b>
<b>BEVEZETÉS .....</b>	<b>108</b>
<b>A MÓDSZERTAN ALAPJAI .....</b>	<b>109</b>
COMMON CRITERIA (CC) ÉS COMMON EVALUATION METHODOLOGY (CEM) .....	110
CWA 14170, CWA 14171, IETF RFC 3280 ÉS 2004. ÉVI LV. TÖRVÉNY .....	113
IETF RFC 3275 ÉS ETSI TS 101 903 .....	115
<b>VIZSGÁLATI ESETEK .....</b>	<b>119</b>
COMMON CRITERIA (CC) ÉS COMMON EVALUATION METHODOLOGY (CEM) .....	119
VIZSGÁLATI ESETEK: CWA 14170, CWA 14171, IETF RFC 3280 ÉS 2004. ÉVI LV. TÖRVÉNY .....	125
IETF RFC 3275 ÉS ETSI TS 101 903 .....	131
<b>VIZSGÁLATI ESETEK ÖSSZERENDELÉSE .....</b>	<b>135</b>
<b>CWA 14170 – RÉSZLETEZÉS .....</b>	<b>136</b>
<b>CWA 14171 – RÉSZLETEZÉS .....</b>	<b>163</b>
<b>A COMMON CRITERIA VÉDELMI PROFILBÓL LEVEZETETT KÖVETELMÉNYEK .....</b>	<b>175</b>
<b>TESZTESETEK .....</b>	<b>243</b>