Europeiska unionens råd

Bryssel den 9 mars 2018
(OR. en)

15082/17
COR 1 (sv)

EF 320
ECOFIN 1053
DELACT 239

FÖLJENOT

från:	Jordi AYET PUIGARNAU, direktör, för Europeiska kommissionens generalsekreterare
inkom den:	8 mars 2018
till:	Jeppe TRANHOLM-MIKKELSEN, generalsekreterare för Europeiska unionens råd
Komm. dok. nr:	C(2018) 1517 final
Ärende:	RÄTTELSE till KOMMISSIONENS DELEGERADE FÖRORDNING (EU) …/… av den XXX om komplettering av Europaparlamentets och rådets direktiv 2015/2366 vad gäller tekniska tillsynsstandarder för sträng kundautentisering och gemensamma och säkra öppna kommunikationsstandarder

För delegationerna bifogas dokument – C(2018) 1517 final.

EUROPEISKA
KOMMISSIONEN

Bryssel den 7.3.2018
C(2018) 1517 final

RÄTTELSE

av den 7.3.2018

till kommissionens delegerade förordning av den 27 november 2017 om komplettering av Europaparlamentets och rådets direktiv 2015/2366 vad gäller tekniska tillsynsstandarder för sträng kundautentisering och gemensamma och säkra öppna kommunikationsstandarder

(C(2017) 7782 final)

RÄTTELSE

till kommissionens delegerade förordning av den 27 november 2017 om komplettering av Europaparlamentets och rådets direktiv 2015/2366 vad gäller tekniska tillsynsstandarder för sträng kundautentisering och gemensamma och säkra öppna kommunikationsstandarder

(C(2017) 7782 final)

I skäl 6 ska det

i stället för: ”För att säkerställa att den stränga kundautentiseringen tillämpas är det också nödvändigt att föreskriva tillräckliga säkerhetsegenskaper hos de element i den stränga kundautentiseringen som kategoriseras som kunskap (något som endast användaren vet), t.ex. längd eller komplexitet, för de element som kategoriseras som innehav (något som bara användaren har), t.ex. algoritmspecifikationer, nyckellängd och entropi, och hos utrustning och programvara som läser element som kategoriseras som unik egenskap (något som användaren är), t.ex. algoritmspecifikationer, skydd för biometriska sensorer och mallar, i synnerhet för att minska risken att dessa element lämnas ut till eller röjs används av icke auktoriserade parter. Det är också nödvändigt att fastställa krav som säkerställer dessa elements oberoende, så att en överträdelse i fråga om ett element inte äventyrar den anordning med flera funktioner, såsom en tablett eller mobiltelefon som kan användas både för att ge betalningsinstruktioner och i autentiseringsförfarandet.”

vara: ”För att säkerställa att den stränga kundautentiseringen tillämpas är det också nödvändigt att föreskriva tillräckliga säkerhetsegenskaper hos de element i den stränga kundautentiseringen som kategoriseras som kunskap (något som endast användaren vet), t.ex. längd eller komplexitet, för de element som kategoriseras som innehav (något som bara användaren har), t.ex. algoritmspecifikationer, nyckellängd och entropi, och hos utrustning och programvara som läser element som kategoriseras som unik egenskap (något som användaren är), t.ex. algoritmspecifikationer, skydd för biometriska sensorer och mallar, i synnerhet för att minska risken att dessa element röjs, lämnas ut till och används av icke auktoriserade parter. Det är också nödvändigt att fastställa krav som säkerställer dessa elements oberoende, så att en överträdelse i fråga om ett element inte äventyrar de andra elementens tillförlitlighet, i synnerhet om något av dessa element används med hjälp av en anordning med flera funktioner, såsom en tablett eller mobiltelefon som kan användas både för att ge betalningsinstruktioner och i autentiseringsförfarandet.”.

Bilaga: C(2018) 1517 final