Sak	Fra	Dokument	Del	Gammel tekst	Forslag til tekst	Evaluering
1044197	Sparebank1	Security Requirements	6.2		Her forstår vi det som at kryptering ikke endres. Ønsker gjerne en bekreftelse på at vi har forstått riktig.	Ingen foreslått endring
1044197	Sparebank1	Security Requirements	6.1		Her forstår vi det slik at det skal signeres (og valideres) med andre algoritmer. Vi lurer dog på motivasjonen for endringen? Gjelder dette sikkerhetshull påpekt av Danske Bank?	Ingen foreslått endring
1044197	Sparebank1	Security Requirements	6.1		Vi og flere andre benytter i dag https://github.com/difi/asic til både kryptering, signering, validering og dekryptering. Vil dette biblioteket kunne brukes videre med disse nye endringene? Vil biblioteket mot formodning oppdateres til å støtte ny standard? Hvis nei, finnes et annet bibliotek det anbefales at man bruker? Går det an å bli enige om et standardvalg som alle i utgangspunktet bruker? (med mulighet for å gå egne veier for de som absolutt vil, selvfølgelig) Kunne til og med et standardvalg blitt dokumentert?	Ingen foreslått endring
1045521	Bits	Security Requirements	6.1.1		Signature suite used: sha3-with-ecdsa Alt 1 (dårligst): rsa-pss with mgf1SHA-256Identifer Alt 2: rsa-pss with mgf1SHA-512Identifier Alt 3 (nest-best): rsa-pss with mgf1SHA3-Identifier	Strykes
1045521	Bits	Security Requirements	6.1.2		Hashing function used: SHA3-256 Alt 1 (dårligst): SHA-256 Alt 2: SHA-384 Alt 3 (nest-best): SHA-512	Strykes
1045521	Bits	Security Requirements	6.1.3		Signature algorithm used: EC-DSA RSA-PSS	Strykes
1045521	Bits	Security Requirements	6.1.4		Minimum 3072 bits key length for RSA keys	Legges til
1045521	Bits	Security Requirements	6.2.2		Signature Scheme: Probabilistic Signature Scheme (PSS) Key encryption with: RSA-OAEP Eventuelt: RSA-OAEP-256	Beholde linje 2
1045521	Bits	Security Requirements	6.2.3		Encryption: AES with 256bit keys. Mode of operation: GCM	Oppdateres
1045521	Bits	Security Requirements	6.2.4		Minimum 3072 bits key length for RSA keys	Legges til
1045742	Bits	Security Requirements	Kapittel 3		Vi forstår ikke tabellen og mener den trenger noe utfyllende/forklarende tekst.	Endres til å være en oversikt over hva som er under endring.
1045742	Bits	Security Requirements	Kapittel 6.2 / kapittel 6		I kap 6.1 står det en timeline for innføring av de nye kravene. Dette er IKKE gjort i kap 6.2. Det burde vel stå timeline her også? Alternativt påpeke at timeline i kap 6.1 gjelder nye krav i både 6.1 og 6.2? (vi tror kanskje det siste er like hensiktsmessig)	Boksen i 6.1 kopieres til 6.2.
1045742	Bits	Security Requirements			Nye og gamle krav – overlappende? Det er satt opp nye krav i kap 6. Samtidig ser vi at krav 5.1.12, 5.1.13 og 5.1.14 er delvis eller helt overlappende. Hel overlappende krav bør slettes. Delvis overlappende krav bør flyttes til kap 6	Fjerne overlappende krav i 5.1.