チェンジリクエスト提案書

［提出者］

提案日		2015 年 1 月 28 日
提案団体		流通システム標準普及推進協議会
連絡先	**氏名:**	梶田 瞳
	所属:	一般財団法人 流通システム開発センター 流通システム標準普及推進協議会
	電話番号:	03-5414-8505
	Email:	*****@dsri.jp

［チェンジリクエスト内容］

CRのタイトル	流通業界共通認証局 証明書ポリシーの改定
目的	技術動向への対応から、流通BMS利用者が使用する証明書ならびにCRLへの署名アルゴリズムを新しいものに変更をし、共通のセキュリティレベル（信頼性）を損なうことなく移行を実施する。
概要	・流通業界共通電子証明書ポリシーにおける署名アルゴリズムのsha2RSA2048bitへの変更と移行についての提案 ・同署名アルゴリズムのsha1RSA2048bitの使用の終了期限の明確化 ・合わせて新規に発行するエンドエンティティについてはRSA2048bit以上とすることを明記
対象物および該当箇所	「流通業界共通認証局 証明書ポリシー第4.0版」 6.1.5. 鍵サイズ 7.1.3. アルゴリズムオブジェクト識別子 表 8 CRL プロファイル
備考	*※本チェンジリクエストを検討する上でのリスクや前提条件等あれば記入すること。* エンドエンティティのRSAの鍵長について、新規発行を2048bit以上に限定することについて、現状とのかい離がないこと

※チェンジリクエストの詳細について資料を添付すること。

以下は事務局にて記入

受付日	2 0 1 5 年 1 月 2 9 日
受付担当者	流通システム標準普及推進協議会 事務局 坂本 真人
CR管理No.	2015-01-001
CR採否	全会一致で承認（2015.02.26開催の技術仕様検討部会にて）
採否の理由	一般的なセキュリティ動向を鑑み、流通BMSとしてもより高度なセキュリティを採用する事が必要と判断した。また、その際に円滑に対応が行われる為の各種周知方法も整理されたため。
採否決定の組織	技術仕様検討部会

以上