



Усиленная электронная подпись

Технология РКІ

Федеральное бюджетное учреждение
«Научный центр правовой информации
при Министерстве юстиции Российской Федерации»

06.03.2015

Атака типа «посредник»

Шаг	Алиса	Меллори	Боб
1	$\sigma^{a \rightarrow}$	σ^a	
2	$\sigma^{n \leftarrow}$	σ^n	
	σ^{an}	σ^{an}	
3		$\sigma^{m \rightarrow}$	σ^m
4		$\sigma^{b \leftarrow}$	σ^b
		σ^{mb}	σ^{mb}

Сертификация ключей проверки подписи



Управление сертификатами

Реестр сертификатов ключей проверки подписи

Действующие сертификаты



Приостановленные сертификаты



Отозванные сертификаты (СОС)

Удостоверение авторства



?

?

Контроль целостности сообщения

