Усиленная электронная подпись

Технология PKI

Федеральное бюджетное учреждение
«Научный центр правовой информации
при Министерстве юстиции Российской Федерации»
06.03.2015

Атака типа «посредник»

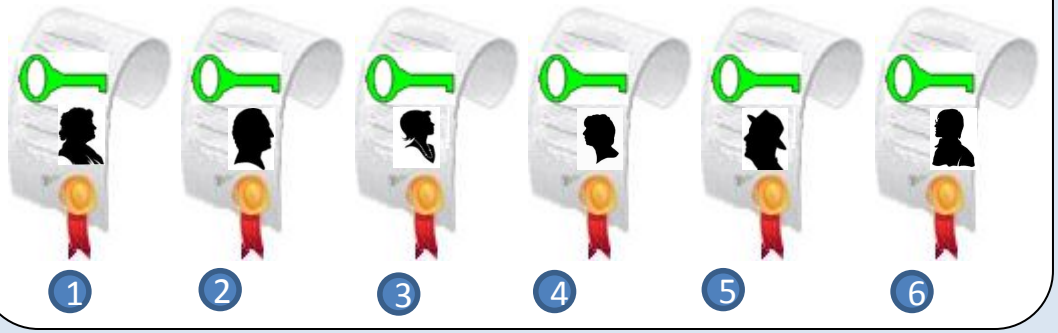
Шаг	Алиса	Меллори	Боб
1	$g^{a\rightarrow}$	g^{a}	
2	$g^{n\leftarrow}$	g^{n}	
	g^{an}	g^{an}	
3		$g^{m\rightarrow}$	g^{m}
4		$g^{b\leftarrow}$	g^{b}
		g^{mb}	g^{mb}

Сертификация ключей проверки подписи

Управление сертификатами

Реестр сертификатов ключей проверки подписи

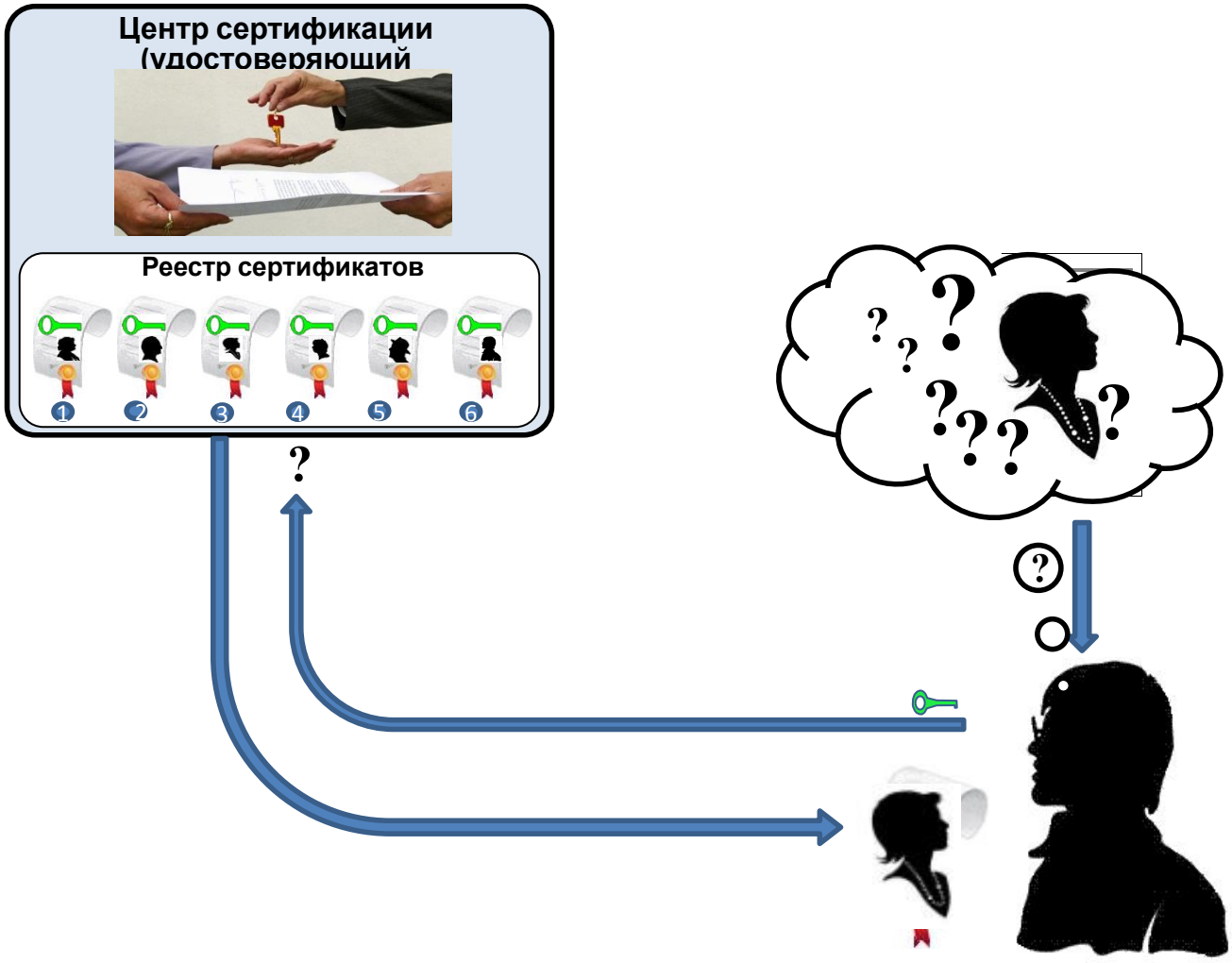
Действующие сертификаты



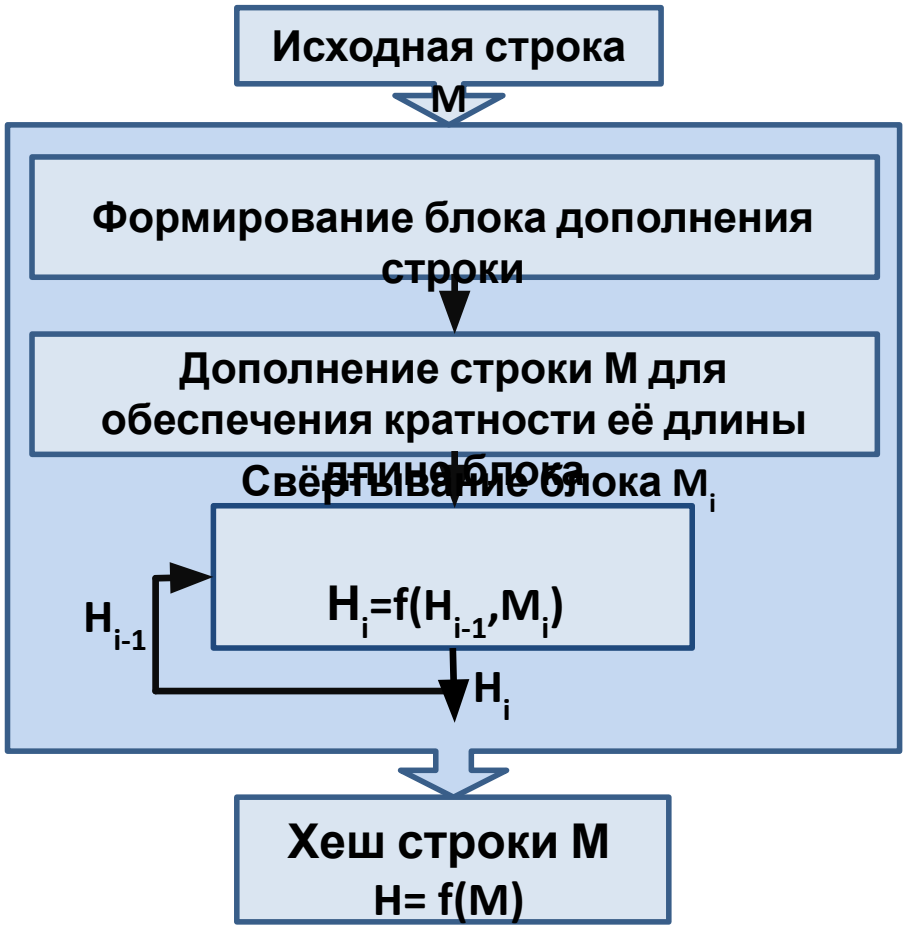
Приостановленные
ртифи

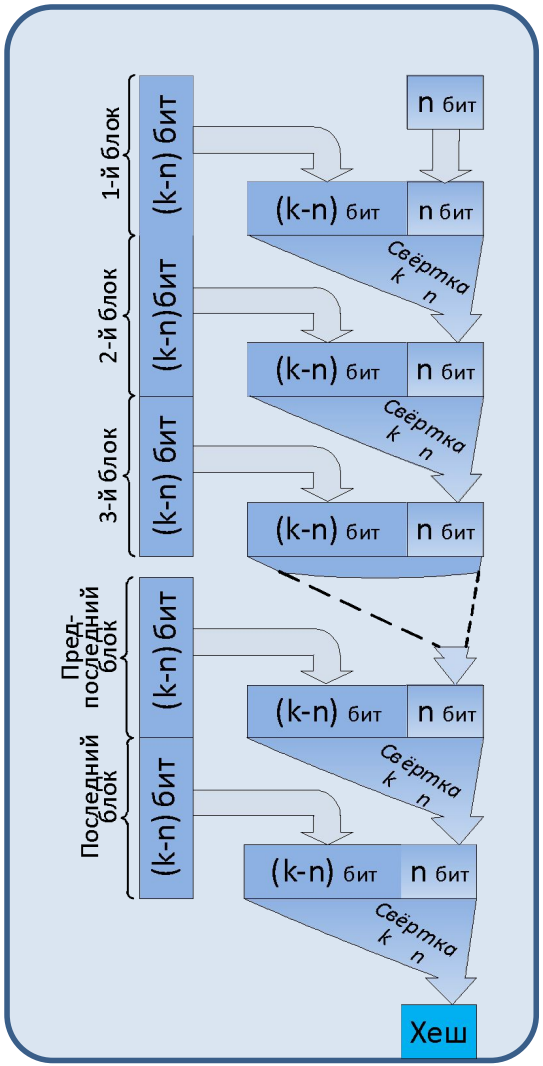
Отозванные сертификаты (СОС)

Удостоверение авторства



Принципиальная схема хеширования





Контроль целостности сообщения