



# Криптографические плагины для браузеров

**Смирнов Павел**  
**Зам. начальника отдела разработок, к.т.н.**  
**ООО «КРИПТО-ПРО»**

© 2000-2015 КРИПТО-ПРО





# Применение криптографических плагинов



## Где применяются

- Электронные торговые площадки
- Порталы государственных услуг
- Интернет-банкинг

## Для чего применяются

- Аутентификация пользователя
- Создание/проверка ЭП
- Зашифрование/расшифрование

# Веб – недоверенная среда



- JavaScript выполняется в «песочнице», но...
- Плагин – проход в стене песочницы



# От чего должен защищать плагин

## Угрозы:

- Блокировка токена/смарткарты
- Чтение локальных файлов
- Чтение сертификатов пользователя
- Использование закрытого ключа
  - Подпись, расшифрование




# Кого иссследовали

## Вендор №1

**СПИСОК ДЕМО-ПЛОЩАДОК**

**ЗАГРУЗИТЬ**

---

 [Плагин для браузера](#)

**ПЕРЕЙТИ К ДЕМО** 

## Вендор №2

**Подключите токен к компьютеру**

Для работы с демонстрацией подключите USB-токен или смарт-карту к Вашему компьютеру. Для подключения смарт-карты требуется наличие смарт-карт ридера.

**ОТМЕНА**

## Вендор №3

**ВОЙТИ ПРИ ПОМОЩИ**

[Средства электронной подписи](#)

# Что плохого обнаружили



Угроза	Вендор №1 	Вендор №2 	Вендор №3 
Блокировка токена/смарткарты	Да	Да	Да
Чтение локальных файлов	Нет	При ПИН-коде по умолчанию	Нет
Чтение сертификатов пользователя	Да	Да	Да
Подписание документов	При запомненном ПИН-коде или по умолчанию	При ПИН-коде по умолчанию	При запомненном ПИН-коде или по умолчанию









**СПАСИБО ЗА ВНИМАНИЕ!**

**КРИПТО-ПРО – ключевое слово в защите информации**

<http://www.cryptopro.ru>

[info@cryptopro.ru](mailto:info@cryptopro.ru)

[spv@cryptopro.ru](mailto:spv@cryptopro.ru)

Тел./факс:

**+7 (495) 995-48-20**