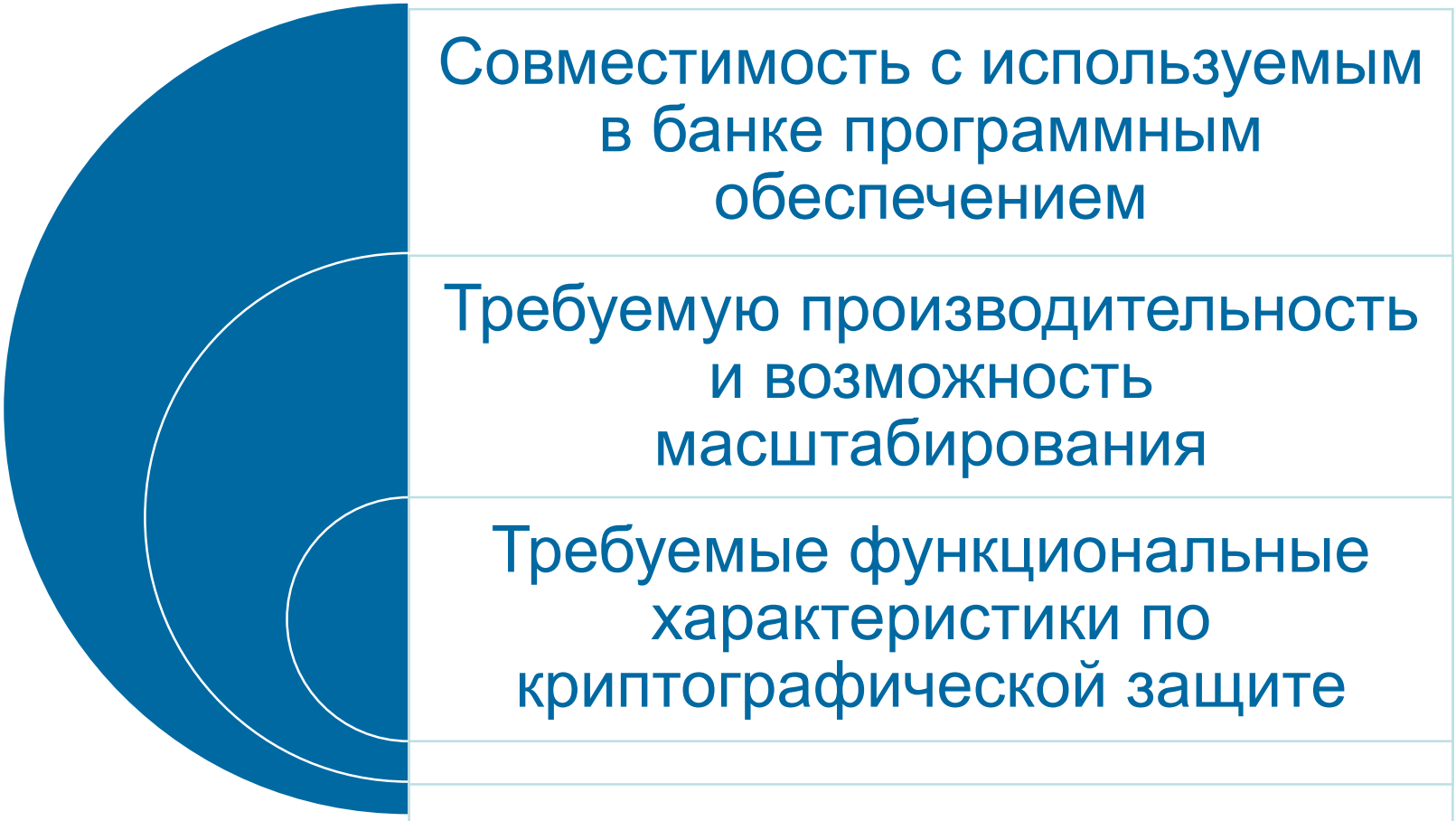
Особенности применения платёжных HSM в процессинговых банковских системах

Заместитель генерального директора
по научно-технической работе
ООО «Системы практической безопасности»
Мареева Елена Владимировна

Требования банков к платёжным HSM

Платёжный HSM должен обеспечивать:



Совместимость с используемым банковским ПО

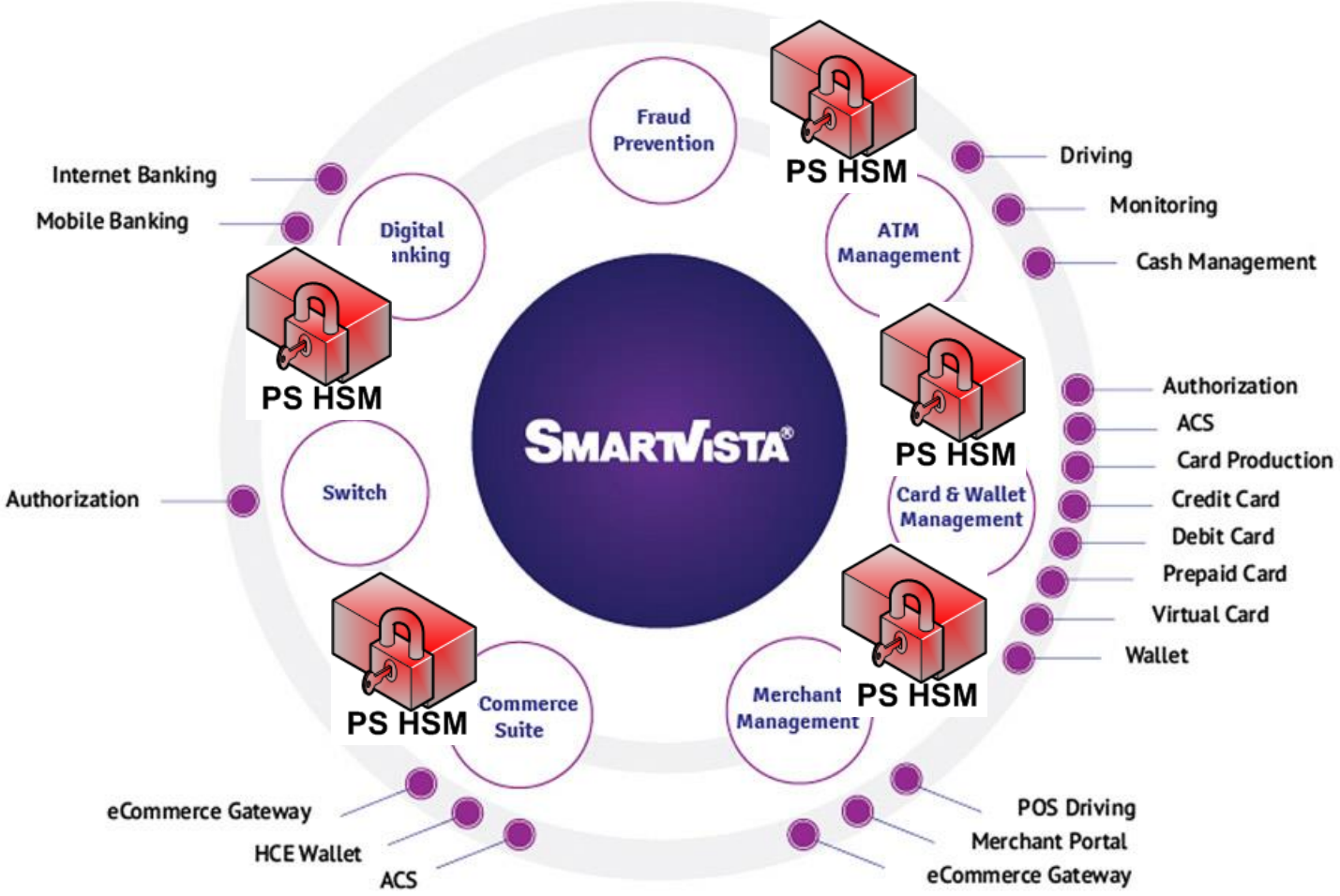
WAY4

Семейство продуктов SmartVista

Линейка TranzWare

Комплексное решение по персонализации EMV-карт

Совместимость с используемым банковским ПО



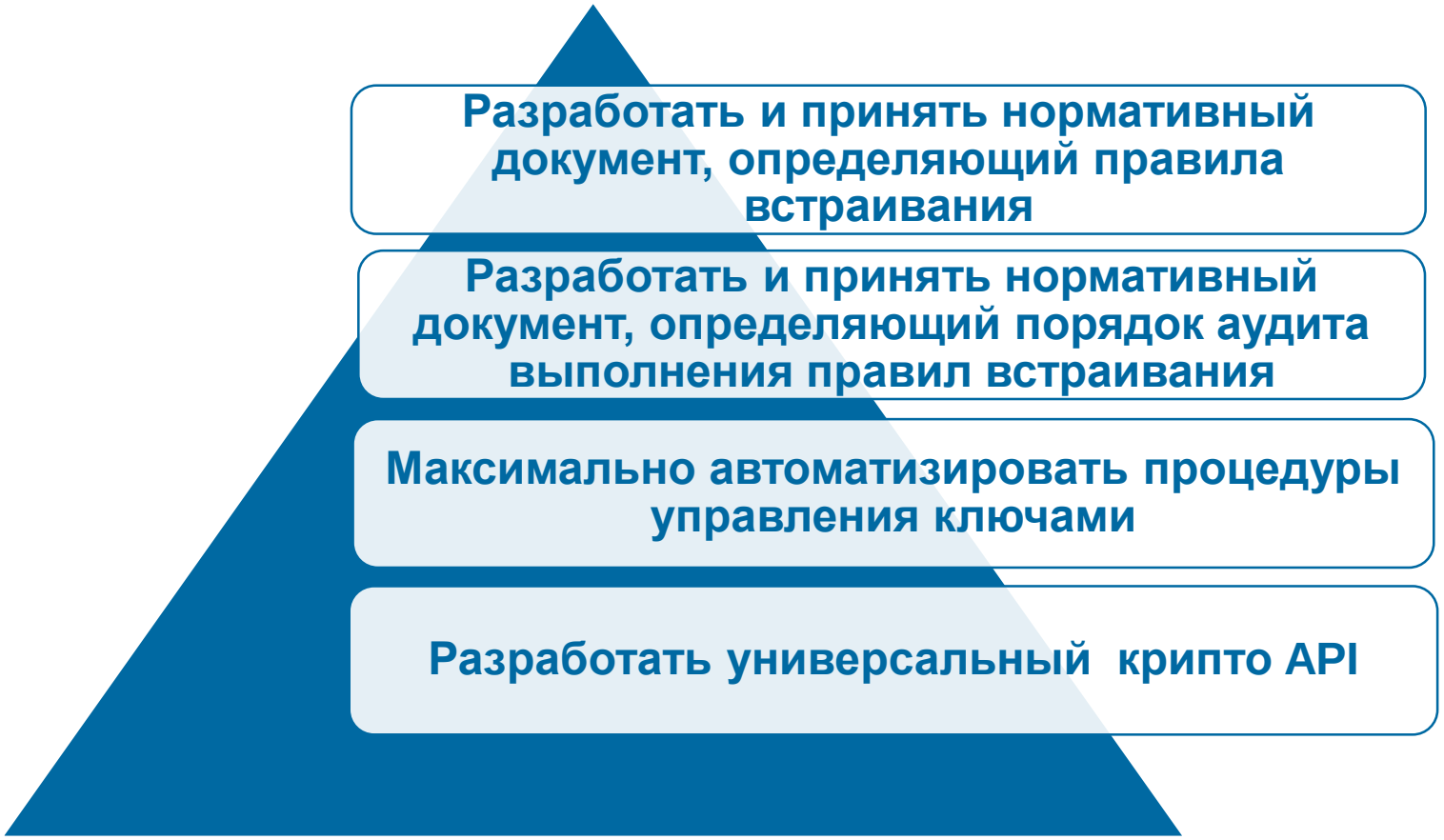
В чём сложности встраивания

	Сложность
1.	Отсутствие универсального API у PS HSM разных производителей
2.	Отсутствие решений по кластеризации
3.	Отсутствие чётких требований по правилам встраивания. PSI DSS определяет лишь общие требования по защите данных держателей карт
4.	Многовариантность решения целевых функциональных задач
5.	Отсутствие знаний в области Key Management и отсутствие стимулов автоматизации процессов в этой области
6.	Отсутствие квалифицированного и обученного персонала в области построения систем криптографической защиты
7.	Отсутствие общих целей и задач, решаемых разработчиками ПО и PS HSM

сложности рождают проблемы

	Сложность	Проблемы
1.	Отсутствие универсального API у PS HSM разных производителей	Огромная трудоёмкость в реализации и тестировании, зависимость от производителя
2.	Отсутствие решений по кластеризации	Эксплуатационные ошибки. Клонирование HSM с одинаковыми LMK
3.	Отсутствие чётких требований по правилам встраивания. PSI DSS определяет лишь общие требования по защите данных держателей карт (ДДК) и критичные аутентификационные данные (КАД)	Показная безопасность, всё, что не касается основных функциональных процессов, делается без учёта требований
4.	Многовариантность решения целевых функциональных задач	Принимаемые технические решения не оптимальны и дороги
5.	Отсутствие знаний в области Key Management и отсутствие стимулов автоматизации процессов в этой области	Смена ключей – процесс практически не выполнимый в высоконагруженной системе
6.	Отсутствие квалифицированного и обученного персонала в области построения систем криптографической защиты	Ошибки в проектировании и , как следствие, во внедрении решений
7.	Отсутствие общих задач, решаемых разработчиками ПО и PS HSM	ПО отстаёт во внедрении новых механизмов защиты, реализованных в PS HSM

Что делать?


Разработать и принять нормативный документ, определяющий правила встраивания
Разработать и принять нормативный документ, определяющий порядок аудита выполнения правил встраивания
Максимально автоматизировать процедуры управления ключами
Разработать универсальный крипто API

ПРОВЕРЕНО PCI DSS

		Элемент данных	Хранение разрешено	Привести хранимые данные к нечитаемому виду согласно требованию 3.4
Данные платежных карт	ДДК	Номер карты (PAN)	Да	Да
		Имя держателя карты	Да	Нет
		Сервисный код	Да	Нет
		Дата истечения срока действия карты	Да	Нет
	КАД[2]	Полные данные треков[3]	Нет	Нельзя хранить согласно требованию 3.2
		CAV2/CVC2/CVV2/CID[4]	Нет	Нельзя хранить согласно требованию 3.2
		ПИН-код и (или) ПИН-блок[5]	Нет	Нельзя хранить согласно требованию 3.2

Требования 3.3 и 3.4 PCI DSS применяются только к PAN. Если PAN хранится вместе с другими элементами ДДК, то согласно требованию 3.4 PCI DSS приводить к нечитаемому виду необходимо только PAN.

После авторизации хранить КАД запрещено (даже в зашифрованном виде). Данное требование действует, даже если PAN отсутствует в среде. Организациям следует связаться со своими эквайерами или напрямую с конкретными международными платежными системами, чтобы узнать, разрешается ли хранить КАД до авторизации, в течение какого срока, а также узнать о соответствующих требованиях к использованию и защите данных.

Спасибо за внимание!

Заместитель генерального директора
по научно-технической работе
ООО «Системы практической безопасности»
Мареева Елена Владимировна

ООО «Системы практической безопасности»,
г. Санкт-Петербург, ул. Шателена, д.26, лит. А, офис 6.18,
www.systempb.ru,
mareeva@systempb.ru,
+7 (812) 468-15-61