IX Уральский форум «Информационная безопасность финансовой сферы»
(Республика Башкортостан, «Юбилейный», февраль 2017 г.)

Обеспечение доверия в информационных технологиях. Практика стандартизации

НПФ «КРИСТАЛЛ»

Почему мы говорим о понятии «доверие» в информационных технологиях и их безопасности

- В последние 20-30 лет применительно к ИТ и их безопасности термин «гарантии» (*эквиваленты: warranty, guarantee и т.п.*) в стандартах не применяется. Это иная область (органы сертификации, зак-во и пр.).
- Для формирования условий обеспечения «гарантии» той или иной стороной применяются стандартизированные подходы и методы обеспечения «доверия» (*эквивалент: assurance*) [*в заданной/ требуемой функциональности, в безопасности, надежности и т.п.*].
- Свидетельства обеспечения доверия формируют субъективные ***суждения и смыслы в контексте риск-менеджмента*** и предназначены для снижения оценок рисков до их приемлемого уровня.
- ***«Доверие»*** (сколько необходимо свидетельств для доверия?) как и ***«риск» - понятия субъективные и во многом есть суть одно и то же*** (доверяю – риск низкий, не доверяю – риск высокий).

Терминология. «Гарантии» и «доверие»

ISO/IEC TR 15443-1 «Information technology – Security techniques – Security assurance framework – Part 1: Introduction and concepts» (**ГОСТ Р 54581-2011/ISO/IEC/TR15443-1:2005**)

- **гарантия** (guarantee): См. определение *Гарантийное обязательство* в п. 2.36.
- **доверие** (assurance): Выполнение соответствующих действий или процедур для *обеспечения уверенности* в том, что оцениваемый объект соответствует своим целям безопасности.

  а) основание для уверенности в том, что сущность отвечает своим целям безопасности [ИСО/МЭК 15408-1].
- **уверенность** (confidence): Убежденность в том, что оцениваемый объект будет функционировать в соответствии с заданным или установленным порядком (то есть, корректно, надежно, эффективно, в соответствии с политикой безопасности).

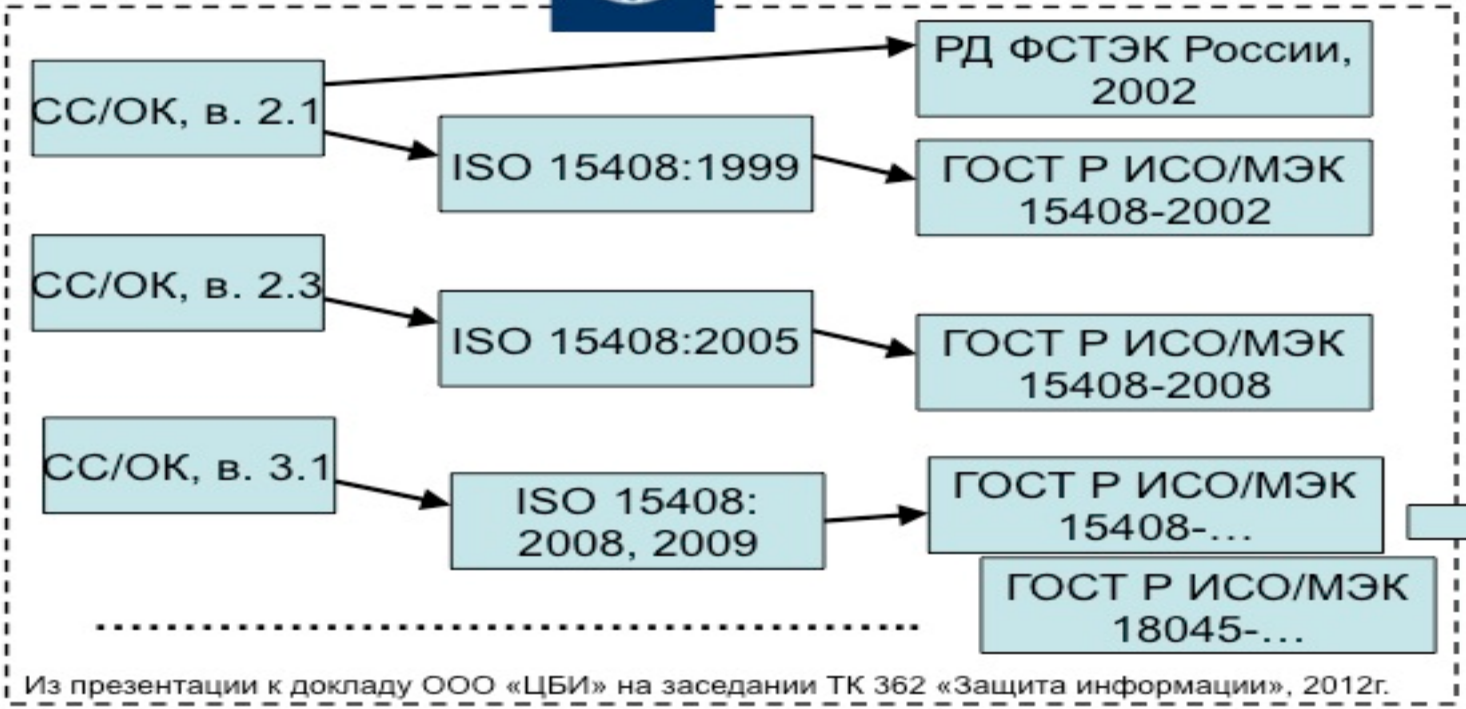
Терминология и понятия области «доверие»

ISO/IEC TR 15443-1 «Information technology – Security techniques – Security assurance framework – Part 1: Introduction and concepts» (**ГОСТ Р 54581-2011/ISO/IEC/TR15443-1:2005**)

- **свидетельство обеспечения доверия** (assurance evidence): Документированные результаты, представленные данными, полученными при анализе доверия к оцениваемому объекту, включая отчеты (обоснования) в поддержку утверждения о доверии.
- ***подход к обеспечению доверия*** *(assurance approach):* **Группирование методов** обеспечения доверия в соответствии с исследуемым аспектом

Одним из наиболее известных подходов к обеспечению доверия к безопасности продуктов ИТ являются так называемые «Общие критерии» (**Common criteria**) или они же – **ИСО/МЭК 15408**

Доверие в безопасности. «Общие критерии»/ИСО 15408 и их применение в РФ



Состав (части) стандарта ГОСТ Р ИСО/МЭК 15408

ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО/МЭК 15408-3— 2013

Информационная технология

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. КРИТЕРИИ ОЦЕНКИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Часть 3

Компоненты доверия к безопасности

ISO/IEC 15408-3:2008
Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components
(IDT)

Издание официальное

ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО/МЭК 15408-2— 2013

Информационная технология

ОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. КРИТЕРИИ ОЦЕНКИ БЕЗОПАСНОСТИ ФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

сть 2 Функциональные компоненты безопасности

ISO/IEC 15408-2:2008
Information technology — Security techniques — criteria for IT security — Part 2: Security functional components
(IDT)

Издание официальное

ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО/МЭК 15408-1— 2012

ационная технология

РЕДСТВА ОБЕСПЕЧЕНИЯ ЗОПАСНОСТИ. ценки безопасности ционных технологий

Часть 1

ние и общая модель

ISO/IEC 15408-1:2009
Security techniques — Evaluation criteria for IT
rt 1: Introduction and general model

(IDT)

Издание официальное

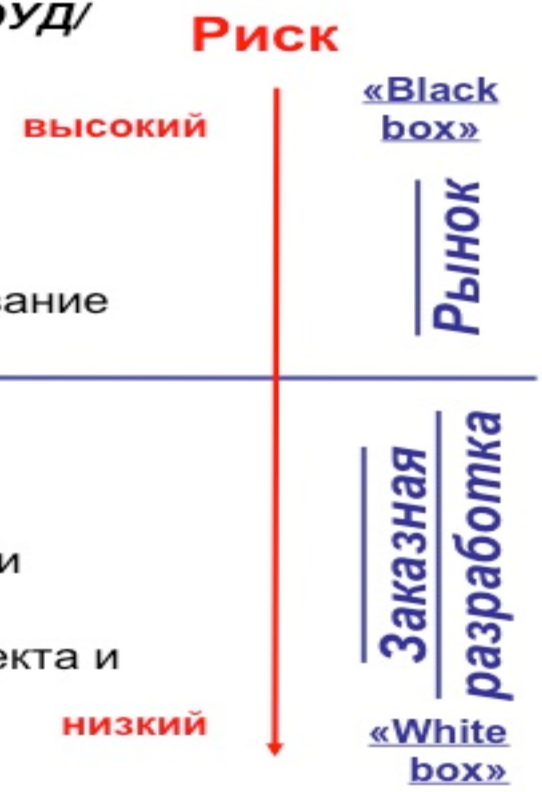
Но это далеко НЕ все «инструменты» используемое в этой технологии

Наименования оценочных уровней доверия «Общих критериев» (ГОСТ Р ИСО/МЭК 15408-3)

Оценочные Уровни Доверия/Evaluation Assurance levels (***ОУД/EAL***)

- ***ОУД1/EAL1*** – Функциональное тестирование;
- ***ОУД2/EAL2*** – Структурное тестирование;
- ***ОУД3/EAL3*** – Методическое тестирование и проверка;
- ***ОУД4/EAL4*** – Методическое проектирование, тестирование и углубленную проверку;

- ***ОУД5/EAL5*** – Полуформальное проектирование и тестирование;
- ***ОУД6/EAL6*** – Полуформальная верификация проекта и тестирование;
- ***ОУД7/EAL7*** – Формальная (строгая) верификация проекта и тестирование;



Состав требований (шкала) оценочных уровней доверия «Общих критериев» (ГОСТ Р ИСО/МЭК 15408-3)

Класс доверия	Семейство доверия	Компоненты доверия из оценочного уровня доверия						
		ОУД1	ОУД2	ОУД3	ОУД4	ОУД5	ОУД6	ОУД7
Разработка	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Руководства	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Поддержка жизненного цикла	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Тестирование	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	2	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Оценка уязвимостей	AVA_VAN	1	2	2	3	4	5	5

Оценочные Уровни Доверия 1 ÷ 7

Пример. Применение «Общих критериев» в платежной индустрии. Европейский платежный совет

European Payments Council

EPC020-08 08.12.2015

(VOL REF. 7.4.2.1)

SEPA CARDS STANDARDISATION (SCS) "VOLUME"

BOOK 4

SECURITY REQUIREMENTS

Payments and Cash Withdrawals with Cards in SEPA

Applicable Standards and Conformance Processes

3.6 Security Requirements For Card Environments

3.6.1 Security Requirements for Physical Chip Cards

This section describes the generic security requirements for Physical Chip Cards. It details the following:
• Scope of Evaluation, outline what parts and functions of the Chip Card are to be evaluated;
• Security Objectives and Assurance Level, outline of main security requirements.

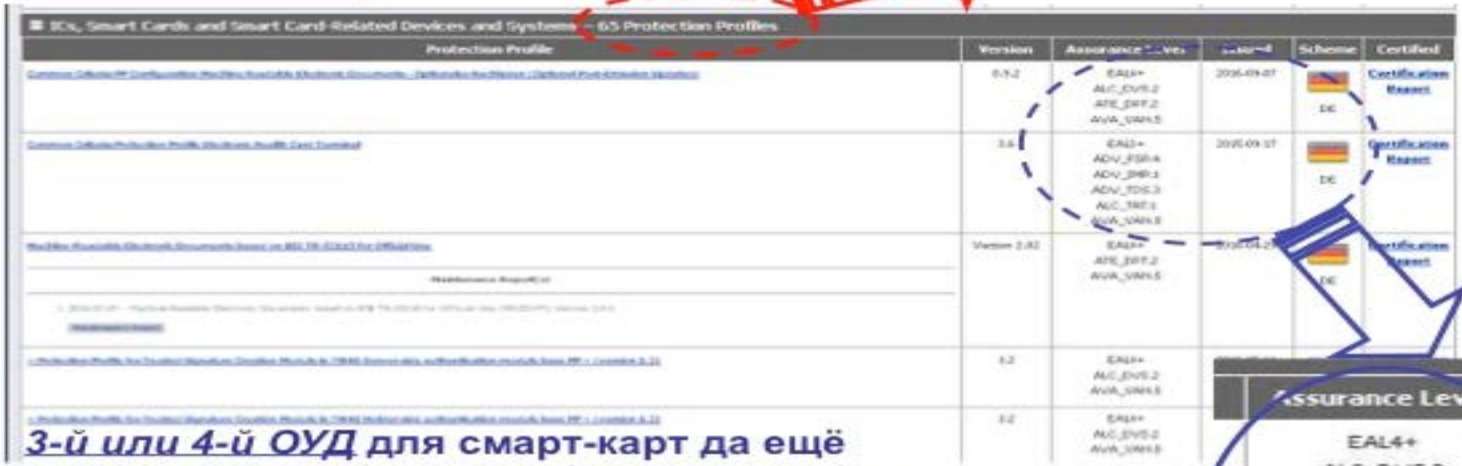
3.6.1.3 Assurance level

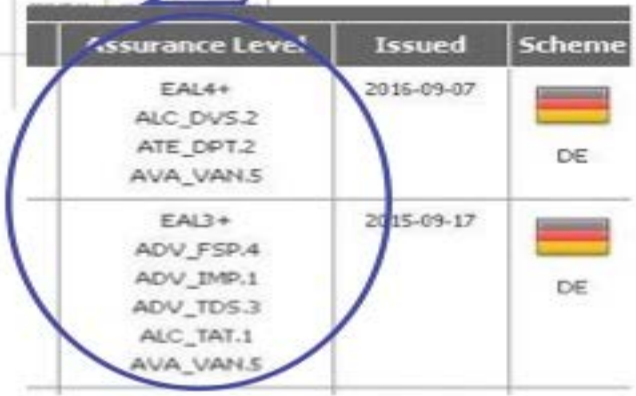
The assurance level to be associated with the Security Objectives listed above for Chip Cards shall be equivalent to the assurance package defined ***as EAL4 in the Common Criteria methodology***. Nevertheless an EAL4 set of assurance requirements shall be augmented respecting……

Реестр сертифицированных профилей защиты. Требования к Смарт-картам, сопутствующим устройствам и системам

Common Criteria

65 Protection Profiles





3-й или 4-й ОУД **для смарт-карт да ещё усиленный («+») – *это обычная зарубежная практика* для подобного типа ИТ-продуктов, сопутствующих устройств и систем.**

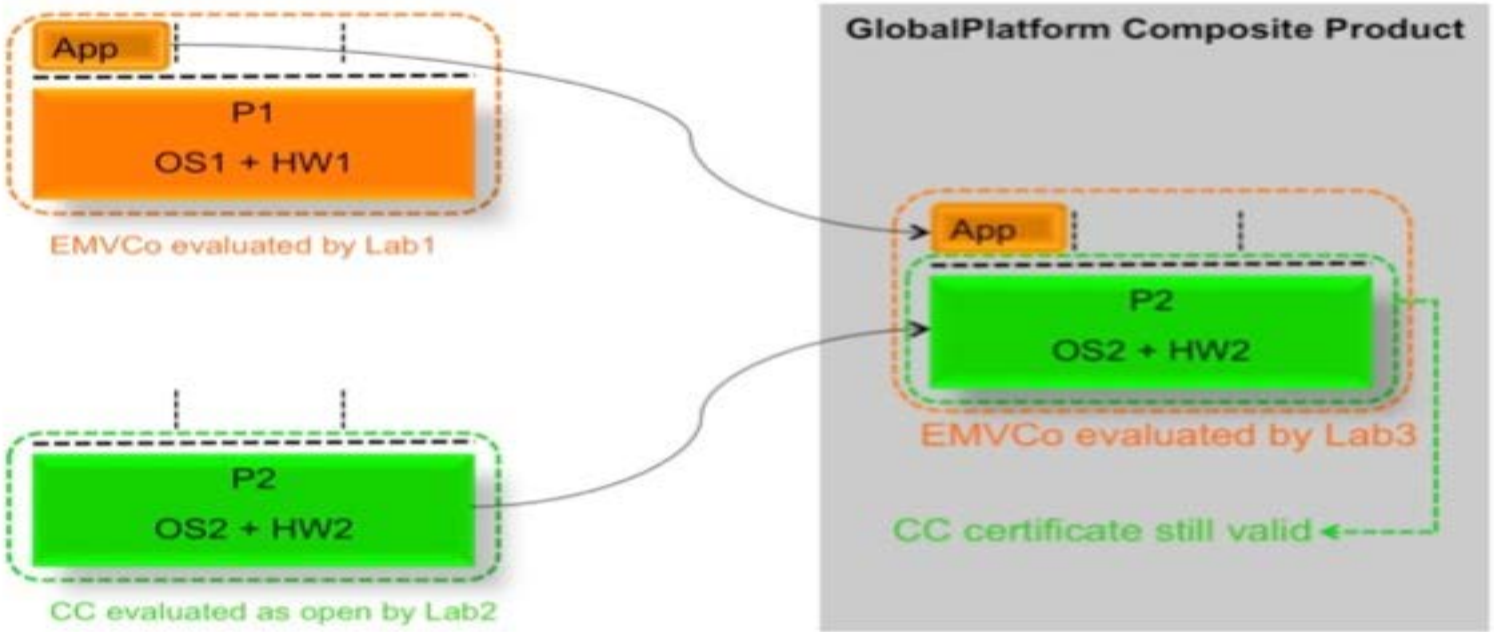
Отечественная в этой части - доподлинно НЕ известна

http://www.commoncriteriaportal.org/pp_IC.html#IC

Пример. Применение «Общих критериев» в платежной индустрии. Ассоциация GlobalPlatform

GlobalPlatform Composition:

ПО сертифицировано по EMVCo, а «железо» и ОС - по «Общим критериям»



GlobalPlatform Card Composition Model. Version 1.1. Public Release. June 2012. Document Reference: GPC_SPE_031

Терминология (продолжение). Прикладной контекст. Доверие [ИБ]

Модель классификации стадий и методов обеспечения «доверия» (ГОСТ Р 54581-2011/ISO/IEC/TR15443-1:2005)

Стадия обеспечения доверия (assurance stage): Стадия жизненного цикла оцениваемого объекта, на которой используется заданный метод обеспечения доверия. *При обеспечении общего доверия к оцениваемому объекту учитываются результаты реализации методов обеспечения доверия, применяемых на всех стадиях его жизненного цикла.*

Пример. Применение различных стандартизированных методов доверия в платежной индустрии.

Схема из результатов исследовательских работ НПФ «Кристалл»

Доверие [безопасности] и технологии идентификации и аутентификации. Действующие стандарты

- NIST 800-63 «Electronic Authentication Guideline»;
- **ISO/IEC 29115 / ITU-T X.1254 «Information technology — Security techniques — Entity authentication assurance framework»;**
- ISO/IEC 29003 «Information technology – Security techniques – Identity proofing»;
- ITU-T Y.2702 «Global information infrastructure. Internet protocol aspects and next-generation networks. Next Generation Networks. Security. Authentication and authorization requirements for NGN release 1»;
- ……..

ISO/IEC 29115 / ITU-T X.1254. Доверие/уверенность при идентификации и аутентификации

- **подтверждение идентификационного атрибута (identity proofing):** Процесс, посредством которого орган регистрации (RA) собирает и подтверждает достаточное количество информации для идентификации сущности с определенным или оговоренным уровнем доверия. [ISO/IEC 29115]
- **аутентификация (authentication):** Обеспечение доверия к идентификационным атрибутам сущности. [ISO/IEC 29115/ ISO/IEC 18014-2]

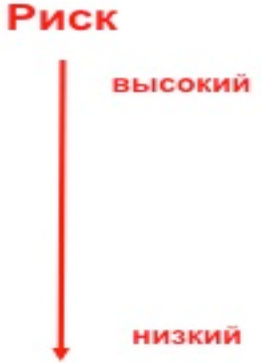
Понятие «доверие» - ключевое для 2-х приведенных выше видов операций

Шкала (уровни) «доверия» к результатам аутентификации (по ISO/IEC 29115)

Уровни доверия (основываются на свидетельствах) [ISO/IEC 29115/ITU-T Recommendation X.1254]

Level	Description
1 – Low	Little or no confidence in the claimed or asserted identity
2 – Medium	Some confidence in the claimed or asserted identity
3 – High	High confidence in the claimed or asserted identity
4 – Very high	Very high confidence in the claimed or asserted identity

Уровень	Описание
1 – Низкий	***Небольшая или нулевая уверенность*** в заявленном или представленном идентификационном атрибуте.
2 – Средний	***Некоторая уверенность*** в заявленном или представленном идентификационном атрибуте.
3 – Высокий	***Высокая уверенность*** в заявленном или представленном идентификационном атрибуте.
4 – Очень высокий	***Очень высокая уверенность*** в заявленном или представленном идентификационном атрибуте.



ISO/IEC 29115 «Entity Authentication Assurance Framework»

Основные области (этапы), применительно к которым рассматриваются меры защиты для соответствующих уровней доверия относительно угроз безопасности

	Технические	Управленческие и организационные
Этап регистрации	• Заявление и инициирование • Подтверждение идентификационных атрибутов и верификация идентификационной информации • Ведение учета/фиксирование	• Организация услуг • Соответствие правовым и договорным требованиям • Финансовое обеспечение • Менеджмент и аудит информационной безопасности • Компоненты внешних услуг • Операционная инфраструктура • Измерение операционных возможностей
Этап менеджмента мандатов	• Создание мандатов • Выпуск мандатов • Активация мандатов • Хранение мандатов • Приостановка, аннулирование и/или уничтожение мандатов • Пролонгация и/или замена мандатов • Ведение учета	
Этап аутентификации сущности	• Аутентификация • Ведение учета	

Рассмотрим далее

ISO/IEC 29115 «Entity Authentication Assurance Framework» (продолжение)

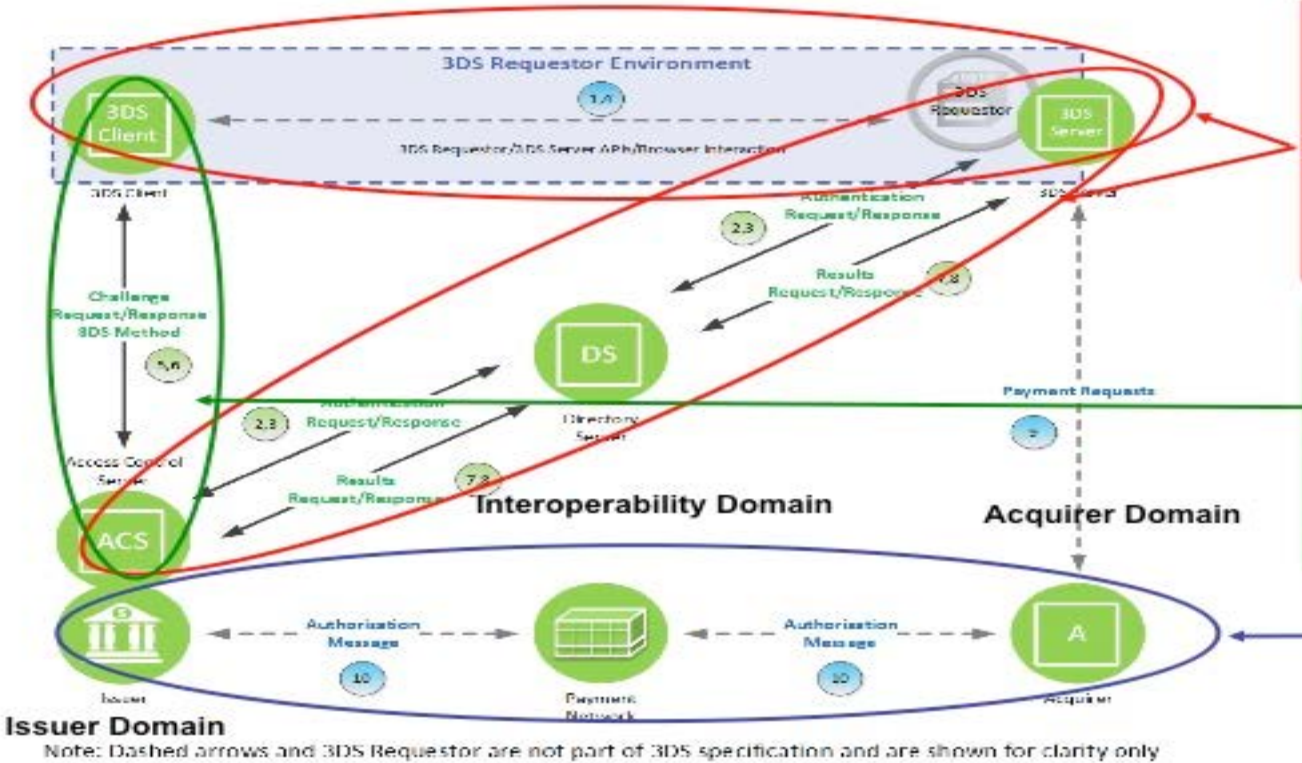
Угрозы и меры и средства контроля и управления для «Этапа аутентификации сущности»

Угрозы	Меры и средства контроля и управления	Требуемые меры и средства контроля и управления				
		УД*	УД1	УД2	УД3	УД4
Общие угрозы**	**Многофакторная-аутентификация**	◢	◢	◢	#1	#1
Онлайновое-отгадывание	Стойкие-пароли Блокирование-мандатов Использование-учетных-записей-по-умолчанию Аудит-и-анализ	#2 #3 #4 #5	◢	◢	◢	◢
Офлайновое-отгадывание	Хэшированные-пароли-с-солью	#6	◢	◢	◢	◢
Дублирование-мандатов	Защита-от-подделок	#7	◢	◢	◢	◢
Фишинг	Обнаружение-фишинга-из-сообщений Принятие-практических-приемов-защиты-от-фишинга **Взаимная-аутентификация**	#8 #9 #10	◢	◢	◢	◢
Подслушивание	Отсутствие-передачи-паролей Зашифрованная-аутентификация Различные-параметры-аутентификации	#11 #12 #13	◢	◢	◢	◢
.....	.....	...	...	...	...	...

** - не всем **«Общим угрозам»** можно противостоять с помощью многофакторной аутентификации
◢ - применение тех или иных «мер и средств контроля и управления» *определяется на основе результата оценки рисков*

Примеры из платежной индустрии. EMV®. 3-D Secure. «Protocol and Core Functions Specification»

3-D Secure. Области и Компоненты



Note: Dashed arrows and 3DS Requestor are not part of 3DS specification and are shown for clarity only

По сути - односторонняя 2-х факторная аутентификация:

Сторона – держатель карты

Факторы:
- первый фактор – группа данных карты
- второй фактор – Одноразовый пароль

Служебный обмен: «Одноразовый пароль» или др, данные.

2-а других сценария не предполагают такого обмена, а основываются на Оценке рисков («скоринговый подход»)

Авторизация платежа

EMV®. 3-D Secure. «Protocol and Core Functions Specification». Version 2.0.0, October 2016

Примеры из платежной индустрии. 3-D Secure. Оценки результатов реализации.

- В результате применения 3-D Secure администрации платежных систем ожидали 4-х кратного снижения объемов потерь от мошенничества
- Не все ожидания оправдались
- По оценке некоторых администраций сокращение произошло лишь двукратное

Идентификация и аутентификация при удаленном взаимодействии

Завершающий слайд многих презентаций Председателя ИСО/МЭК/СТК1 «Информационные технологии» ПК27 «Методы и средства обеспечения безопасности»

Lessons Learned

- "On the Internet, nobody knows you're a dog."
- "eBusiness (eGovernment, ...) will not evolve without appropriate security solutions."
- "Secure systems are 10% about security technology and 90% about organization."
- "Trust is good – control is better."
- "Standards connect the world."

"On the Internet, nobody knows you're a dog."

© Из коллекции New Yorker. 1993г.

Выделено:

- **В Интернет никто НЕ знает что я собака!**

Спасибо за внимание!

В.Б. Голованов
Зам. научного директора

НПФ «КРИСТАЛЛ»
г. Пенза

Email: crystall@sura.ru
www.npf-crystall.ru