

ТЕХНОЛОГИЯ НАДЕЖНОЙ ИДЕНТИФИКАЦИИ ЛИЦ, ПРЕДМЕТОВ И ДОКУМЕНТОВ, И ВОЗМОЖНЫЕ ВАРИАНТЫ МОНЕТИЗАЦИИ ЕЕ ВНЕДРЕНИЯ В РАЗЛИЧНЫХ СФЕРАХ.

Многие процессы в нашей жизни требуют проверки подлинности и актуальности на текущий момент. И эта ситуация востребована и при прямом контакте (например, убедиться в подлинности предъявленного документа, а также в его актуальности на момент предъявления; подлинности товара и т.п.), и уж просто незаменима при удаленном взаимодействии, в первую очередь через Интернет.

В обычной жизни для этих целей используются разные способы в зависимости от потребности, например:

для удостоверения личности в общем случае – документы, выданные государством (паспорт, водительские права и т.п.), а для допуска лиц в ограниченную зону – пропуск;

для удостоверения подлинности предметов: упаковка с описанием; различные элементы защиты (голограммы, стикеры и т.п.).

для защиты документов – чисто внешние атрибуты (бумага с защитой, синие или красные печати, закорючки подписей и т.п.).

Но для эффективного использования этих способов защиты проверяющему лицу необходимо обладать определенными знаниями: как отличить настоящий документ, удостоверяющий личность, от поддельного?; как отличить настоящую голограмму от поддельной?; как удостовериться что подпись и печать на документе настоящие? Соответствуют ли элементы полиграфической защиты бланка эталонным? И т.д. и т.п. ...

Практически, только единицы людей, и то из числа профессионалов, обладают такими знаниями. На практике, только эксперт может определить подделку. Но ведь эксперт появляется уже на стадии СОСТОЯВЕШЬСЯ ситуации – совершения злоупотребления (как правило – мошенничества), основанного на фальсификации информации (в документе, на предмете, в предъявленном удостоверении личности, паспорте).

Но, кроме проблемы определения **подлинности** личности, предметов и документов, существует и другая проблема – определение **актуальности** этих свойств на текущий момент! Иными словами, **подлинная** доверенность с **подлинной** подписью и печатью – может быть аннулирована буквально час назад! А предъявленное **подлинное** удостоверение личности (паспорт, служебное и т.п.) – числится **утерянным** или **аннулированным**, т.е. **неактуальным**. Ну а при изготовлении поддельных товаров основным моментом является максимально точное копирование упаковки...

Как ВЫВОД: решить проблему надежной идентификации личности и предметов (с учетом актуальности как при прямом контакте, так и при удаленном взаимодействии) существующими ныне способами при существующем порядке вещей – **весьма проблематично**.

Проанализировав, все существующие системы идентификации и защиты (в первую очередь экспертный доклад «Анализ систем защиты от подделок» от Информационно-Аналитического Агентства «Антиконтрафакт»), изучив достоинства и недостатки практически всех существующих систем и технологий (как в обычной, так и в электронной жизни), мы пришли к выводу, что создать возможность надежной идентификации лиц, предметов и документов (а также их актуальности на момент проверки) – **ВОЗМОЖНО** ! Но только на базе современных инфотехнологий. Приступая к теоретической разработке такой системы, мы поняли, что в современном мире достаточно динамично происходит перемещение личностей, предметов и документов через границы, и локальное решение (в рамках одной страны) не может быть эффективным. Следовательно, для получения должной эффективности необходимо решать этот вопрос в глобальном измерении, то есть в рамках универсальной трансграничной системы идентификации личности, предметов и документов.

За предыдущие три года нашей команде удалось создать такую технологию!

Мы создали технологию с рабочим названием GRIPTDS «Global Reliable Identification Of People, Things and Documents System» («Глобальная надежная система идентификации лиц, вещей и документов»). Не вдаваясь в технические нюансы (достаточно обозначить, что в основе этого решения лежит гармоничное использование криптографии и технологии электронной подписи), мы с полной ответственностью можем утверждать, что более гармоничного с точки зрения удобства и надежности способа идентификации (с учетом актуальности!) на сегодняшний день не существует!

Результатом работы технологии GRIPTDS является: с одной стороны – получение заинтересованным лицом при проведении им проверки предъявленного документа или вещи в режиме «онлайн» **достоверной** информации из **надежного** источника в **юридически значимом виде**, на основании которой можно сделать обоснованный вывод о подлинности личности, предметов, документов. А также об актуальности этих свойств на момент проверки!

С другой стороны, любая подключенная к сервису информационная система (банковские и почтовые сервисы; социальные сети; платные информационные ресурсы; развлекательные ресурсы; пропускные системы; системы парковки и т.д. и т.п.) – может получить достоверную и актуальную информацию о лице, с которым вступает во взаимодействие удаленным образом, в том числе и при осуществлении им проверки подлинности вещей, товаров и документов.

Также, при удаленном взаимодействии лицо может подписать электронной подписью (на уровне «усиленной») любую информацию, предоставленную информационной системе.

И не имеет значения в какой юрисдикции находится информационная система и лицо, взаимодействующие между собой.

Такие возможности в настоящий момент не может дать ни одна из существующих аналогичных систем.

* * *

Границы возможностей применения разработанной технологии мы сами еще до конца не осознали. Причем, выгодоприобретателями будут и бизнес, и государство, и самое главное – потребители и пользователи.

Вот краткий список того, что мы увидели в первом приближении:

1. Предотвращение мошенничеств с использованием фальсифицированных или неактуальных документов.

2. Решение проблем со сбытом фальсифицированной и контрафактной продукцией (как через обычные торговые сети, так и через Интернет-магазины) – через многократно возрастающие риски выявления их до покупки и автоматическое информирование об этом владельцев бренда и других заинтересованных лиц). В результате увеличения этих рисков при сбыте, становится экономически невыгодным и ее производство (*Прототип создан - система защиты от подделок «Crypto Contra Counterfeit Protection (CCCP)*).

3. Фиксация перемещения отдельных товарных единиц в составе товарных партий от производителей до конечной точки продажи.

4. Формирование досье жизненного цикла от производства до утилизации (с указанием персональных данных всех причастных к различным этапам лиц) как отдельных изделий из числа комплектующих, так и сложных изделий, состоящих из массы комплектующих;

5. Получение заинтересованными лицами в режиме «онлайн» информации: где, когда, по какой цене и кому именно была продана конкретная оригинальная товарная единица, и аналогичная информация о попытке сбыта фальсификата. (*Уникальный инструмент для маркетинга*).

6. Формирование социального портрета потребителя на основе анализа его предпочтений – также уникальный инструмент для маркетологов.

7. Надежная идентификация личности в электронной среде, полная замена небезопасной системы идентификации по «логин + пароль» и других систем идентификации (в том числе и многофакторных) в интересах неограниченного количества информационных систем (*Прототип создан – система «Welcome Without Password» (WWP)*).

8. Создание альтернативных платежных систем с полным отказом от общепризнанных ненадежных банковских карт. Решение проблем с мошенничествами посредством поддельных сайтов и порталов. Защита денежных купюр (*Ведутся переговоры с ЦБ РФ и рядом других банков*).

9. Обеспечение доступа к хранилищам и помещениям, контроль перемещения и допуска лиц.

10. Противоугонные системы для автомобилей. Организация доступа в помещения (от служебных до личных квартир и домов).

11. Организация оплаты парковки в любой точке мира (концепция разработана).

И еще многое другое, где необходима надежная идентификация, и не только при удаленном взаимодействии, но и при личном контакте...

По нашему мнению, предлагаемая технология может заинтересовать:

1. **Владельцев брендов и производителей оригинальной продукции.** Ведь именно они в первую очередь страдают от наличия на рынке контрафакта и фальсификата (оттягивание большой части потребителей; компрометация бренда из-за низкого качества подделки). Появление у потребителей и участников логистической цепочки легкой, доступной, материально поощряемой возможности легко и надежно отличить оригинал от подделки еще до покупки сделает затруднительным сбыт фальсификата, а следовательно, будет экономически невыгодно и его производство.

2. **Информационные системы** (повышение уровня безопасности, исключение возможности пользоваться их платными услугами для «двойников», имеющих копии логинов и паролей);

3. **Финансовые организации.** Появляется возможность если не полностью исключить хищения денежных средств путем взлома, использования фейковых сайтов и других стандартных манипуляций) то уж, по крайней мере существенно сократить это негативное явление; создание принципиально новых платежных систем, свободных от существующих сейчас угроз и атак.

4. **Маркетологов** (отслеживание цен по местам сбыта и времени, формирование потребительского портрета, возможность прямого взаимодействия с потребителем); Полная замена различных бонусных карт (брендов, магазинов, АЗС и т.п.) на единый инструмент с более широкими возможностями, по сравнению с ныне существующими пластиковыми картами.

5. **Потребителей!** Потому что при правильном внедрении всей системы, основанной на этой технологии, потребителю будет выгодно активно использовать ее на своем мобильном устройстве, т.к. у него появляется возможность не только осуществлять проверку подлинности предлагаемых ему товаров и документов, но и простым и надежным способом идентифицировать себя в любой системе. И на базе таких возможностей вполне реально создать специфическую социальную сеть, которая может стать по количеству пользователей достойным конкурентам Фейсбуку, Twitter, и многим другим.

6. **Государство.** Помимо решения многих проблем, которые сейчас не решены (засилье контрафакта и фальсификата в различных областях, мошенничество с документами и т.п.), государство получает возможность мониторинга движения товаров, его сбыта, цен и других действий с ним в рамках жизненного цикла.