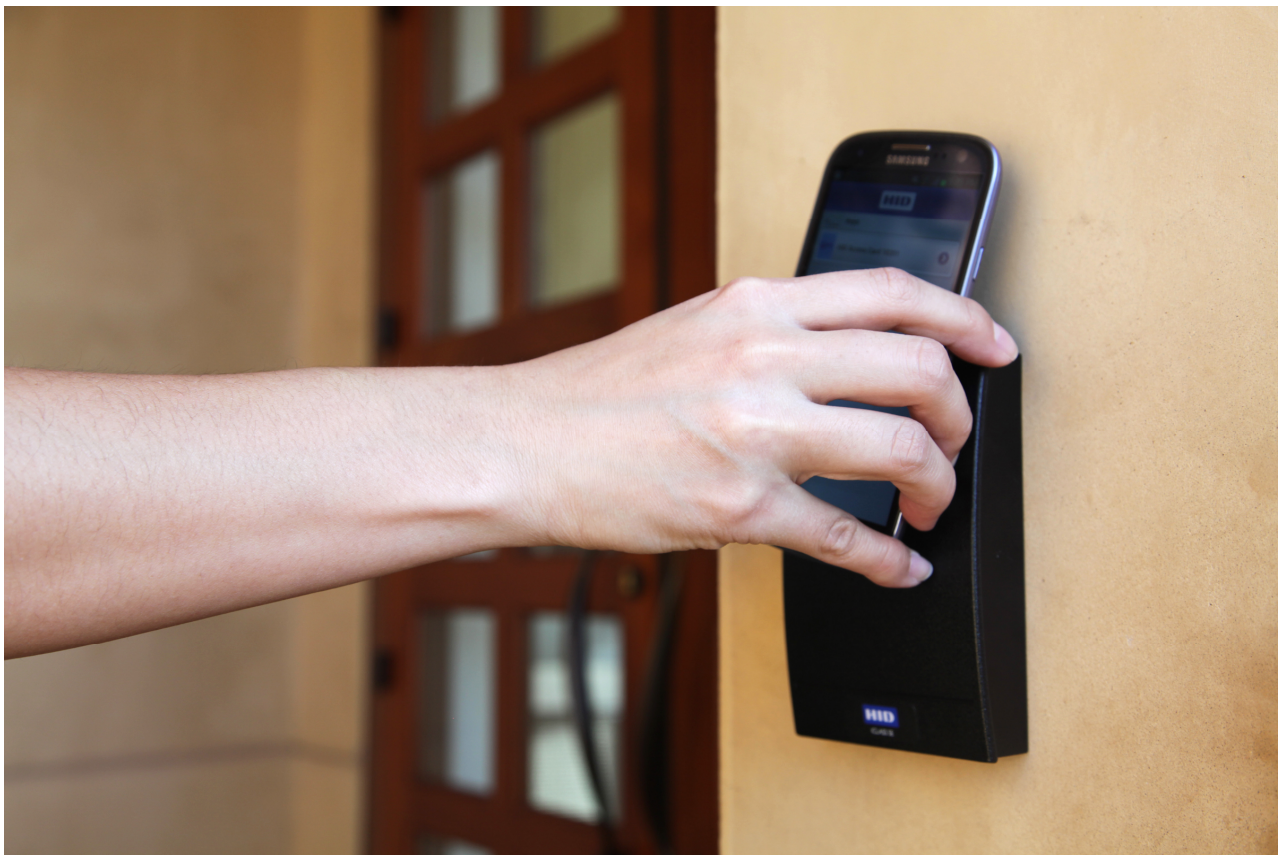
NFC: бесконтактный офис

Беспроводная технология малого радиуса действия NFC (NearFieldCommunication, "коммуникация ближнего поля") является одним из наиболее популярных современных трендов и постепенно становится катализатором использования мобильных устройств как электронных ключей в системах контроля доступа. По принципу действия NFC похожа на технологии Bluetooth и RFID, однако, обладает целым рядом важных конкурентных преимуществ: скорость и уровень безопасности у нее выше, чем у Bluetooth, а функциональные возможности шире, чем у RFID. Несмотря на это, дорога от лаборатории до начала запуска проектов оказалась для NFC достаточно долгой — самой технологии уже 10 лет. Она была принята как стандарт в 2003 году и только в 2011 началось ее постепенное распространение.



В России NFC-сегмент находится на ранней стадии развития, в то время как в западных странах уже накоплен определенный, хотя и не столь обширный, опыт практического использования этой технологии, в частности, в коммерческом секторе для обеспечения контроля доступа. В некоторых странах Европы и США устройства, оснащенные технологией NFC, применяются в системах контроля доступа образовательных учреждений, гостиниц, медицинских комплексов и в коммерческом секторе. К примеру, в офисах пользователи могут получать на свои смартфоны цифровые ключи, дающие им право доступа в различные помещения, а также в зоны для хранения конфиденциальной коммерческой и личной информации. При этом поддерживаются различные уровни безопасности и функции назначения правил доступа.

В России начинают реализовываться первые пилотные проекты по использованию NFC в СКУД – пока это прерогатива только крупных корпораций – однако существует ряд факторов, сдерживающих развитие этой технологии в нашей стране. В первую очередь, сфера контроля доступа, как правило, консервативна и медлительна во всем, что связано с внедрением новых

решений. Это связано не только с защитой данных, но и с интеграцией с различными системами безопасности и необходимостью соответствия определенным регламентирующим правилам. Кроме того, для данной технологии крайне важно развитие соответствующей инфраструктуры, в формирование которой пока не идет достаточный поток инвестиций. Должна быть выстроена экосистема поставщиков услуг, включающая в себя провайдеров телекоммуникационных сервисов, доверенных сервис-менеджеров и других поставщиков услуг, которые могут передавать идентификационные данные и управлять ими.

Немаловажным фактором также является достаточное количество мобильных телефонов с поддержкой NFC для реализации функций мобильного контроля доступа. По прогнозам аналитической компании BergInsight, в период с 2012 по 2017 год рынок телефонов с поддержкой NFC увеличится до 2,1 млрд устройств с совокупным ежегодным темпом роста на уровне 65%. К 2017 году уровень проникновения NFC во всех сегментах рынка телефонов увеличится примерно до 32%.Таким образом, дальнейшее развитие экосистемы и рост числа NFC-устройств будут оказывать первоочередное влияние на то, как быстро технология NFC будет принята для решения различных задач, в том числе в сфере контроля доступа.

Впрочем, несмотря на ряд ограничений, у NFC существует и множество преимуществ, которые буду способствовать тому, что эта концепция рано или поздно, но обязательно завоюет рынок. Используемыйвпределахзащищеннойсистемысмартфонпредоставляетплатформудлясозданиябез опаснойсредымобильнойидентификации, включая защищенный канал для передачи идентификационной информации между доверенными телефонами, их элементами безопасности и другими безопасными устройствами и носителями. Каждые новые идентификационные данные могут быть загружены на смартфон удаленно: пользователи легко могут получать цифровые ключи по сети, а менеджеры по безопасности приобретают возможность дистанционно управлять данными постоянных пользователей или генерировать временные ключи для посетителей. Так, при использовании мобильных ключей работодателю станет гораздо проще отслеживать все активности сотрудников. Кроме того, в подобной системе могут использоваться любые мобильные устройства, и организации не нужно затрачивать средства на приобретение смартфонов – сотрудники могут пользоваться личными телефонами при условии соблюдения основного требования –поддержки смартфоном модуля NFC.

Функции физического и логического контроля доступа также могут совмещаться в NFC-устройствах. Смартфоны будут использоваться для доступа в здание, входа в сеть, запуска приложений, удаленного доступа к защищенным сетям без необходимости ввода одноразового пароля. Подобная конвергенция функций в одном смартфоне NFC позволит повысить удобство для пользователя, уровень безопасности и сократить расходы на внедрение и эксплуатацию.

NFC-устройства способны поддерживать и биометрические шаблоны, что является очень важной характеристикой этой технологии. Если требуется обеспечить повышенный уровень защиты, можно применить биометрию для идентификации пользователя в мобильной системе контроля доступа. Шаблоны биометрических характеристик можно хранить на самом устройстве, и непосредственно устройство следует подносить к специальной распознающей камере для проверки подлинности.

Маловероятно, что мобильный контроль доступа с помощью технологии NFC в ближайшее время полностью заменит собой ключи и карты доступа. Смартфоны NFC будут использоваться наряду с картами доступа и пропусками, а многие организации будут по-прежнему выдавать своим сотрудникам традиционные идентификационные бейджи с фотографией. Однако рынок NFC

имеет огромный потенциал, а универсальность этой технологии и способность решать большое количество задач гарантирует NFC колоссальные перспективы в бизнесе.