munication Union) определяют набор сервисов и услуг, в совокупности составляющих Доверенную третью сторону (ДТС). В списке сервисов ДТС присутствует сервис атрибутирования, пример технической реализации которого приведен в международных рекомендациях RFC 3281.

Данные рекомендации вводят понятие атрибутного сертификата (АС), криптографически однозначно связанного с сертификатом открытого ключа. Атрибутных сертификатов может быть несколько, каждый из которых содержит сгруппированную информацию, определяющую роль ранее идентифицированного субъекта.

Использование атрибутных сертификатов для представления дополнительных данных о пользователе позволит организовать один или несколько тематически разделенных реестров ограниченного доступа, за наполнение которых будут отвечать уполномоченные органы, а прикладные ИС будут выступать только в качестве пользователя услуги по получению ролевой информации из доверенного источника.

В этом случае ДТС фактически будет являться тем "единым окном", через которое происходит официальное наполнение, изменение и получение дополнительной информации о пользователе.

Описанный способ размещения дополнительной информации не накладывает никаких ограничений на способы представления данных внутри прикладных информационных систем. Вместе с тем:

- снимаются проблемы актуальности, целостности и достоверности дополнительной информации;
- полностью исключается влияние изменяющихся потребностей прикладных систем на процедуру издания персональных сертификатов пользователей;
- ввиду стандартности способа публикации процедура присоединения произвольной прикладной ИС становится также стандартной и прозрачной;
- прикладные ИС помимо стандартизированного инструмента для получения дополнительной информации о пользователе от ДТС смогут, используя эту же технологию, более эффективно организовывать взаимодействие между собой;
- вопросы аутентификации и защиты информации, размещаемой в АС, по выбору уполномоченных органов могут решаться любыми апробированными способами (начиная с шифрования АС в адрес легитимного получателя и заканчивая организацией защищенных сетевых соединений).

Идея сервиса атрибутирования лежит в общем русле технологии PKI и является ее естественным развитием и приложением. На данный момент имеются примеры успешного внедрения данного сервиса как для организации разграничения доступа к массивам данных, так и для представления учетных данных пользователей внутри прикладных систем. Более того, в одной из стран ЕС есть пример использования АС совместно с квалифицированными сертификатами. ●

Ваше мнение и вопросы присылайте по адресу
infosec@groteck.ru

Инфраструктура сопровождения жизненного цикла АС и сертификатов открытых ключей очень схожи за тем исключением, что АС не содержат открытого ключа и к их публикации не применимы нормы ФЗ "Об ЭЦП" в части свободного доступа к реестру, где сертификаты будут опубликованы.

Целостность, актуальность и авторство наполнения атрибутов в АС заверяются при помощи ЭЦП службы атрибутирования

Таким образом, возможность применения данной технологии для организации одного из сервисов государственной ДТС выглядит вполне логичной, особенно учитывая возрастающую потребность в подобном решении и повышенное внимание, уделяемое последнее время федеральной целевой программе "Электронная Россия"