ЭЛЕКТРОННЫЙ ДОКУМЕНТООБОРОТ и ЦИФРОВАЯ ПОДПИСЬ

В УСЛОВИЯХ ИСПОЛЬЗОВАНИЯ CAD/CAM-СИСТЕМ КОНСТРУКТОРСКО-ТЕХНОЛОГИЧЕСКОЙ ПОДГОТОВКИ ПРОИЗВОДСТВА

В наши дни технология электронной цифровой подписи (ЭЦП) активно внедряется в организациях, где уже создан электронный архив и работает система электронного документооборота (СЭД). Использование ЭЦП для обычных электронных документов (ЭД), каждому из которых соответствует файл в СЭД, регламентируется Законом РФ "Об электронной цифровой подписи" [1]. В организации, внедряющей ЭЦП, должен быть создан удостоверяющий центр (УЦ) для осуществления поддержки этой технологии и подключения к ней (сертифицирования) сотрудников.

Каждому сотруднику-владельцу ЭЦП, предоставившему доверительное соглашение, в котором он признает за своей ЭПЦ юридическую силу, аналогичную собственноручной подписи, администратор УЦ выдает сертификат. Этот сертификат представляет собой автономный носитель (дискету, флэш-модуль), содержащий уникальный идентификатор владельца (закрытый ключ ЭЦП) для ввода подписи, а также открытый ключ для возможности проверки ЭЦП другими лицами. Открытый ключ формируется на основе закрытого и подписывается владельцем подписи вместе с доверительным соглашением. Технически все процедуры кодирования определены в ГОСТ Р 34.10-2001 [2]. Процесс сертификации нового клиента УЦ условно показан на рис. 1.

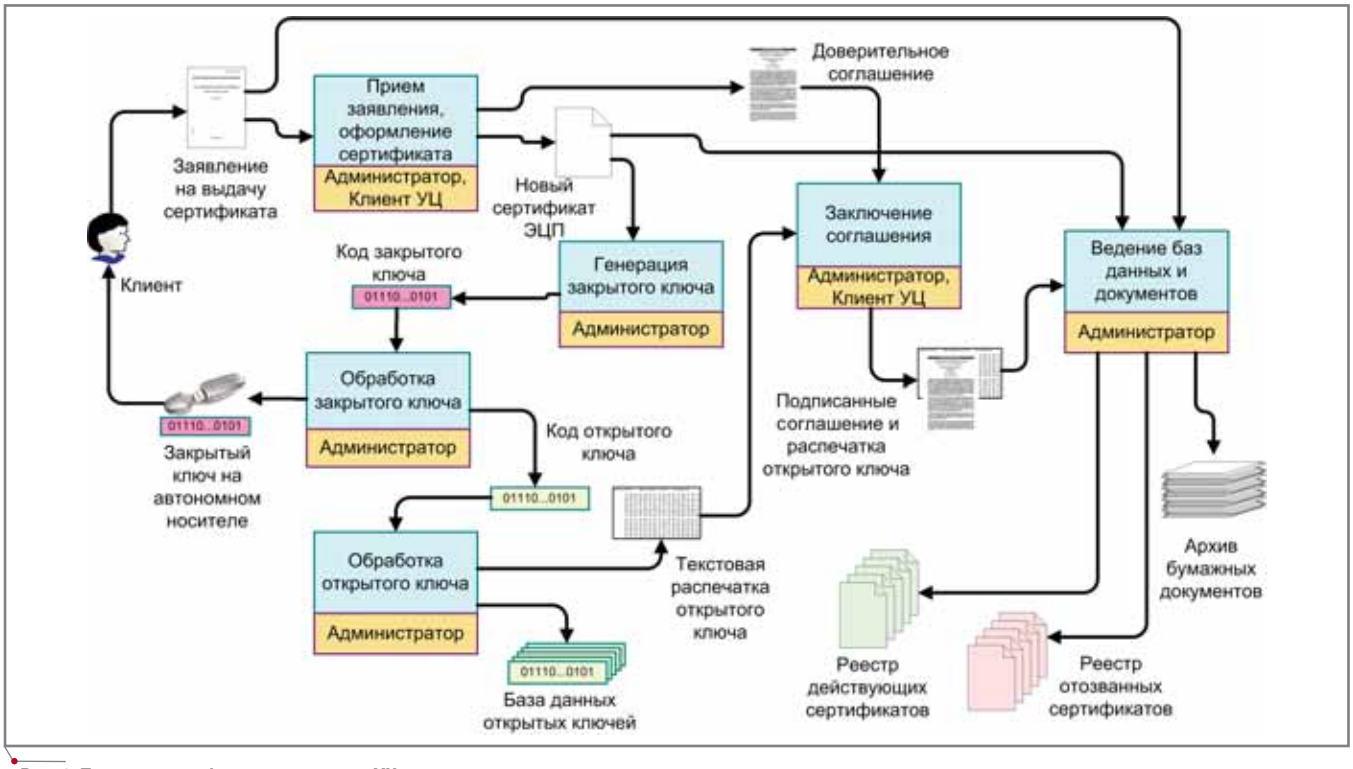


Рис. 1. Процесс сертификации клиента в УЦ

С момента получения сертификата клиент может без ограничений вводить ЭЦП в любые файлы, которые в пределах юрисдикции УЦ будут считаться подписанными. Естественно, уполномоченные лица могут приостанавливать право конкретного пользователя подписывать электронные документы и переводить его сертификат в категорию отозванных. Именно поэтому УЦ всегда предоставляет информацию о действующих и отозванных сертификатах (рис. 1).

Поскольку файлы могут быть сколь угодно большими, технология ввода ЭЦП в соответствии с ГОСТ Р 34.11-94 [3] предполагает их обработку для получения компактного значения (хэш-функции) всего в 32 байта. Вводимая в документ ЭЦП вычисляется на основе этого значения хэш-функции и закрытого ключа, как показано на рис. 2.

В условиях действующего УЦ любая ЭЦП может быть легко проверена на достоверность всеми клиентами СЭД, которая должна располагать соответствующими функциями и иметь базу данных открытых ключей всех пользователей. В процессе проверки подписанного файла СЭД осуществляет его свертку к тем же 32 байтам хэш-функции и производит вычисление на основе открытого ключа владельца ЭЦП, как показано на рис. 3.

Таким образом, если в подписанном файле каким-либо образом изменен или добавлен хотя бы один бит информации, его хэш-функция

Рис. 2. Процедура ввода ЭЦП в файл документа

НОВОСТИ

" CSoft ! (=$ ESG) «/2 % /.
< % % < .
2 % »

Компания CSoft Санкт-Петербург (Бюро ESG) стала одним из организаторов конференции «"Интеграция предприятий". Организационные и технологические схемы электронного взаимодействия участников создания и эксплуатации корабля. Инновационный проект в судостроении», которая состоялась в апреле 2006 г. во ФГУП "ЦНИИ технологии судостроения".

В форуме приняли участие представители таких компаний, как ФГУП "Рособоронэкспорт", ФГУП "ЦНИИ им. академика А.Н.Крылова", 1 ЦНИИ МО РФ, ОАО "Балтийский завод", ГУП "Адмиралтейские верфи" и др.

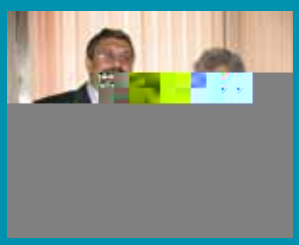
Основными проблемами, рассмотренными на конференции, стали организация работ по созданию электронной информационной модели кораблей (ЭИМК) и использование ИПИ-технологий в рамках инновационного проекта в судостроении.

С большим вниманием был выслушан представленный компанией CSoft Санкт-Петербург доклад "Элементы ИЛП. Технология автоматизированного контроля наименований предметов снабжения" (Бюро ESG) (авторы: В.А. Александров, С.М. Козменко, А.А. Рындин, к.т.н. А.А. Тучков, И.Б. Фертман).

В ходе работы конференции были определены конкретные мероприятия по организации единого информационного пространства при создании сложных изделий на основе типовых унифицированных программно-технических решений. Кроме того, обсуждались вопросы формирования организационных и технологических схем электронного взаимодействия между кораблестроителями и мореходами.

:
.7. - ... &
'4 3 ' '-9,
'. . ' 1 ...)
G-9 7/
"4 95 ",
J. . ...)
3 '
'-9

0 !
. . / ,
! 9(
MSN



6.5. / & , !
))
NOQS, 5.9. 3) ,
! QSoft
' %

. . 9 ! ,
' 3 '
" !) & "

! -9
« »
.7. 7

щественные затраты не позволяют решить главный вопрос – утверждение комплексного решения "модель-документ", поскольку физически подписать файл модели невозможно. Единственным решением проблемы является внедрение СЭД, в которой предусмотрены все средства поддержки технологии ЭЦП, включая УЦ, модули ввода и проверки, как показано на рис. 5.

В данном случае разработчик решения лично предъявляет для утверждения весь комплект файлов со встроенными ЭЦП. Эта технология предусматривает приоритет электронного документа, то есть подлинником считается сам подписанный файл, хотя, естественно, всегда можно получить для просмотра и бумажную копию из архива. С помощью ЭЦП подписываются и утверждаются также и файлы объемных моделей. Предусмотренный для этих целей в СЭД 3D-визуализатор, который может быть запущен на любом компьютере, позволяет любому уполномоченному лицу просматривать в разных ракурсах и масштабах все особенности принятого на модели решения. Внедрение данной технологии может осуществляться только при условии совместной работы СЭД и УЦ, когда все участники процесса сертифицированы и имеют закрытые ключи.

Внедрение СЭД с технологией ЭЦП – важнейший этап технического развития организации, актуальность которого особенно возрастает в связи с изменениями в ЕСКД, где официально признано использование в составе конструкторской документации электронных документов, содержащих модели детали и сборочной единицы (например, в ГОСТ 2.102-68 "Виды и комплектность конструкторских документов").

Несмотря на серьезные материальные затраты, связанные с внедрением СЭД, предлагаемая технология предоставляет предприятию целый ряд преимуществ:

- полное исключение возможности потери документов, их несанкционированного использования третьими лицами;
- существенная экономия времени на согласование и утверждение документов;
- повышение производительности благодаря возможности быстрого и результативного поиска нужных документов, а также прототипов чертежей и техпроцессов;
- сокращение затрат на выдачу копий документов;
- минимизация издержек благодаря повышению качества документов и быстрому доступу к хранилищу.

Эффективное внедрение ЭЦП на предприятии предполагает разработку внутреннего стандарта по статусу электронного документа и технологии ЭЦП. На данный момент такая разработка выполнена совместно компаниями "Глосис-Сервис" и CSoft Санкт-Петербург (Бюро ESG) для санкт-петербургского ОАО "Красный Октябрь", где активно внедряется СЭД с использованием в качестве базового программного обеспечения системы TDMS, поддерживающая технологию объемного проектирования. Применяемые стандарты созданы с учетом самых разнообразных электронных форматов документов и их связи с проектами трехмерного проектирования различных CAD-систем.

>

1. Российская Федерация // Федеральный закон об электронной цифровой подписи. – №1-ФЗ от 10.01.02.
2. ГОСТ Р 34.10-2001 "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи".
3. ГОСТ Р 34.11-94 "Информационная технология. Криптографическая защита информации. Функция хэширования".

Николай Пиликов,
директор ООО "Глосис-Сервис"
Тел.: (812) 542-0469
E-mail: soft@glosys.ru

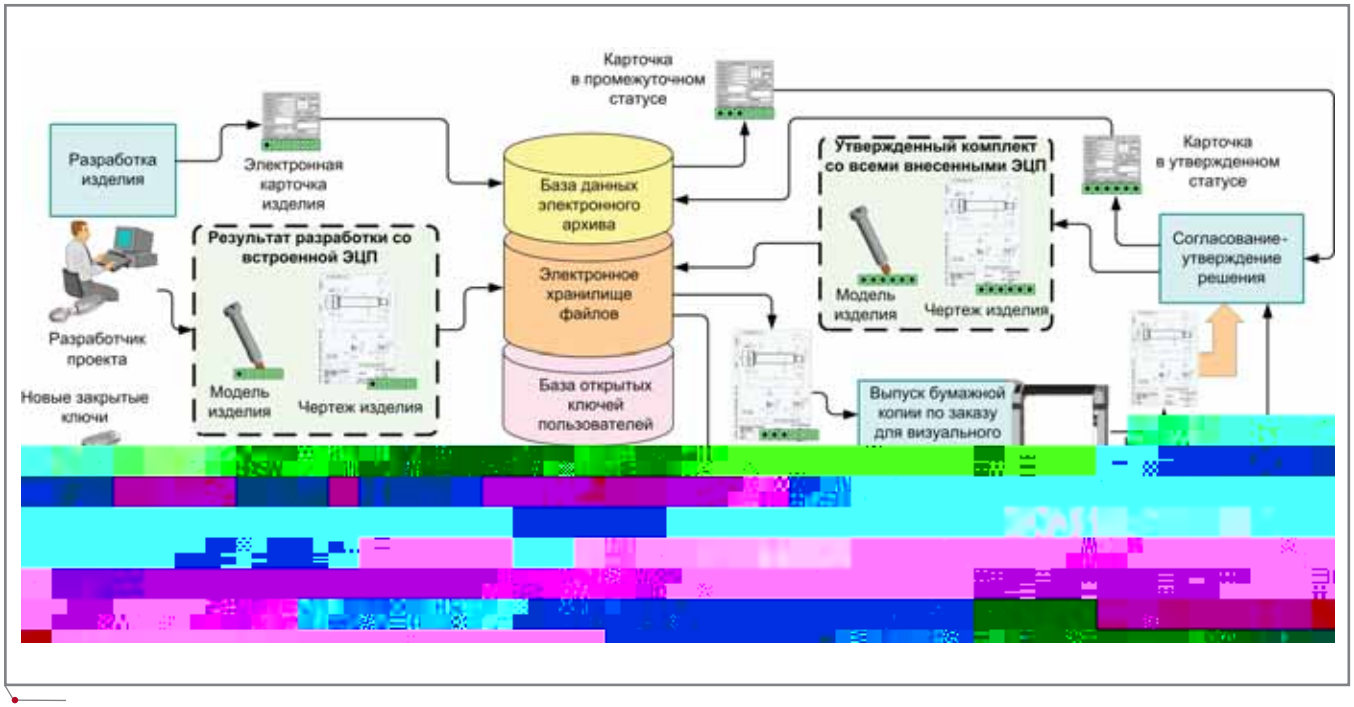


Рис. 5. Схема утверждения комплекта "модель-документ" в условиях использования СЭД и ЭЦП