

СОСТОЯНИЕ И СУЩНОСТЬ ПРОЦЕССОВ НОРМАЛИЗАЦИИ ЕВРОПЕЙСКОЙ НОРМАТИВНОЙ БАЗЫ В ОБЛАСТИ ЭЛЕКТРОННЫХ ПОДПИСЕЙ

Ю.И. ГОРБЕНКО, А.В. ПОТИЙ, А.В. КОСТЕНКО, Е.В. ИСИРОВА, И.Д. ГОРБЕНКО

Рассматриваются процессы нормализации Европейской нормативной базы в области электронных подписей. Анализируются причины осуществления нормализации и результаты выполнения работ. Обсуждается новая схема нумерации документов, а также рассмотрена каждая из предметных областей применения.

Ключевые слова: нормализация европейской нормативной базы в области электронных подписей, электронные доверительные (трастовые) услуги, Мандат 460, структура нормативных документов в ЕС в области электронных подписей.

ВВЕДЕНИЕ

В Европейском Союзе (ЕС) уже 15 лет успешно внедряются и применяются электронные услуги. В соответствии с Директивой 1999/93/ЕС внедрена и успешно применяется электронная цифровая подпись (ЭЦП). Опыт ее применения позволил сделать положительные оценки, а также выявить проблемные вопросы, необходимость ее усовершенствования и развития. Также сделан вывод о необходимости расширении электронных услуг, сделать их в пределах ЕС трансграничными. Результаты исследований и разработок были представлены и утверждены в Регламенте 2012 года [1]. В 2014 году принят Регламент Европейского Парламента и Совета по вопросам электронной идентификации и доверительных услуг (сервисов) для электронных операций на внутреннем рынке (Регламент 2014) [2]. В данном документе расширяется сфера применения ЭЦП. Технология ЭЦП используется для предоставления электронных услуг метки времени и электронной печати. Кроме того, ЭЦП становится основным элементом подтверждения других электронных услуг — электронной идентификации, аутентификации, печати, электронного документа, надежной электронной доставки. В терминологии Регламента 2014 она получила название электронной подписи (ЭП). Широкое применение технологии ЭП обусловило разработку многочисленных стандартов и норм, затрагивающих различные вопросы реализации и использования ЭП. Это способствует унификации и обеспечению надежности средств ЭП. Однако наблюдается и негативный эффект — это несвязность многочисленных нормативных документов и стандартов, дублирование норм. Это, в свою очередь, усложняет ориентацию в массиве документов и корректное их применение разработчиками, регуляторами и сервис-провайдерами электронных доверительных услуг и ЭП (рис. 1). Также формируются новые барьеры на пути дальнейшего расширения и применения электронных доверительных услуг. Все это

можно охарактеризовать некой «болезнью роста», когда система функционально усложняется и требует перехода на новую структуру, отвечающую степени функциональной сложности.

Целью настоящей статьи является анализ нормативного документа, который получил название Мандата 460, в части создания условий для взаимодействия разных систем ЭП на уровне ЕС посредством улучшенной рационализации существующей структуры нормативных документов.

1. СУЩЕСТВУЮЩАЯ СТРУКТУРА И ПРОЦЕСС НОРМАЛИЗАЦИИ НОРМАТИВНЫХ ДОКУМЕНТОВ В ОБЛАСТИ ЭЦП

На рис. 1 структура нормативных документов в области ЭП в ЕС в области ЭП до начала процессов нормализации приведена на рис. 1. Основной проблемой существующей структуры нормативных документов в области ЭП является обеспечение трансграничности даже внутри ЕС. Преодолевая эти и другие проблемы, было принято решение нормализовать и упорядочить нормативную базу.

Упорядочение или нормализация системы нормативных документов ЕС в области ЭП и электронных доверительных услуг осуществляется в рамках так называемого Мандата 460 [3]. Целью разработки и принятия Мандата 460 является создание условий для взаимодействия различных криптографических систем ЭП в ЕС. Эта цель достигается путем рационализации существующей структуры нормативных документов ЕС в области ЭП. Суть процесса нормализации приведена на рис. 2.

Можно увидеть, что множество документов классифицировано согласно определенным критериям. Процесс классификации позволил исключить дублирующие документы, а также дополнить систему недостающими документами. В результате такой классификации выделено семь групп документов. Каждая группа документов описывает определенный аспект применения

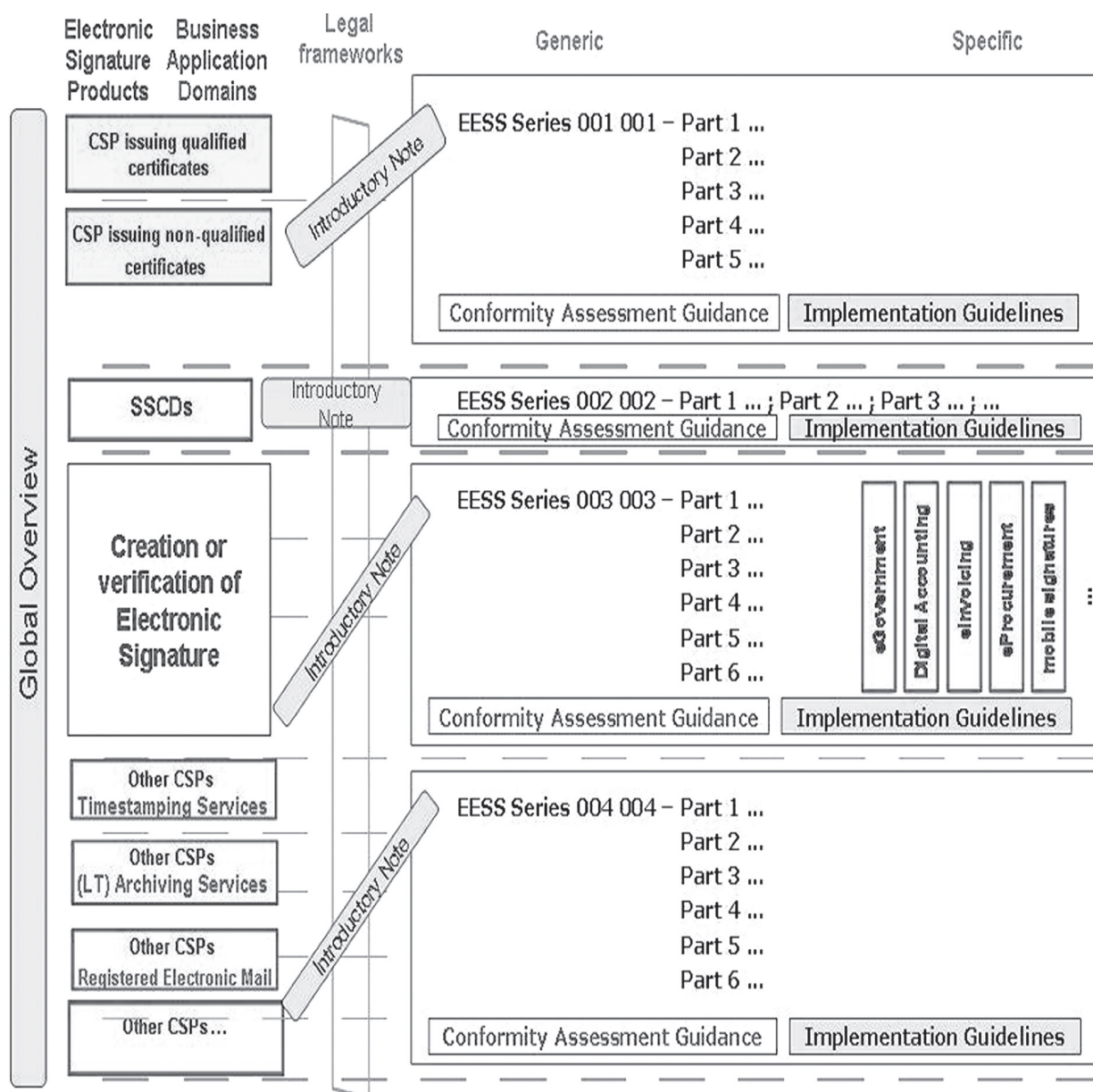


Рис. 2. Суть процесса нормализации нормативных документов в ЕС [4]

требования к системам, которые реализуют технические стандарты.

Технические характеристики систем. Эти документы определяют технические требования к системам и средствам ЭП. Они содержат форматы, протоколы, алгоритмы, API, профили конкретных стандартов и т.д., и не ограничиваются техническими архитектурами, которые описывают стандартизированные элементы системы и их взаимосвязи.

Требования к оценке соответствия требованиям стандартов описывают требования к оценке соответствия систем и средств ЭП требованиям безопасности. Документы содержат правила оценки соответствия, включая общие критерии оценки продукции или оценки систем и услуг и т.д.

Требования к тестовым испытаниям на совместимость. Эти документы содержат требования и спецификации для организации и проведения испытаний на совместимость, порядок



Рис. 3. Семиуровневая система нормативных документов в области ЭП [4]

тестирования систем, а также проведения испытаний или тестирования систем, которые обеспечивают автоматизированную проверку соответствия продукции, услуг или систем [4].

3. ОБОЗНАЧЕНИЕ ДОКУМЕНТОВ

Уникальная нумерация документации мандата 460 была выполнена с целью определения единого и последовательного ряда стандартов ЭП, и обеспечивает отслеживаемость всех модификаций документа за все время его существования.

В мандате 460 используется такая схема нумерации:

DD	L19	xxx	z
----	-----	-----	---

Поле DD указывает на тип соответствующего документа (принимает значения SR, TS, TR и EN);

Поле L19 — идентификатор составляющих частей документа. В данном идентификаторе L=4 — идентифицирует составляющую часть стандарта CEN. L=0, 1, 2 или 3 — идентифицирует составляющую часть стандарта ETSI и тип документа, который установлен в процессе стандартизации. Идентификатор 19 указывает на ряд документов по стандартизации, связанных с ЭП. Приняты следующие идентификаторы: код 019 — специальный отчет ETSI (SR); код 119 — техническая спецификация (TS) и технический отчет (TR) ETSI; код 219 — стандарт (ES) и руководство ETSI (EG); код 319 — Европейские нормы (EN) ETSI; 419 — техническая спецификация (TS) или Европейский стандарт (EN) CEN.

Поле xxx указывает серийный номер (от 000 до 999) документов ETSI/CEN. Первая цифра кода (Xxx) идентифицирует область документа: код 0 — общий для ряда областей; код 1 — создание руководства и проверка подписей; код 2 — устройства создания подписей; код 3 — криптографические комплексы; код 4 — провайдеры трастовых услуг, которые используют электронные подписи; код 5 — провайдеры приложений трастовых услуг; код 6 — список статуса провайдеров трастовых услуг.

Вторая цифра кода (xXx) определяет под-область в идентифицированной области, или 0 для общих документов данной области.

Третья цифра кода (xxX) обозначает тип документа, где: код 0 — руководства, код 1 — требования безопасности и политики безопасности, код 2 — технические характеристики, код 3 — оценка соответствия, код 4 — тестовые испытания и совместимость.

Поле z идентифицирует составные части документов.

Дополнительная нумерация для идентификации частей и версий будет осуществляться в соответствии с конвенциями ETSI или CEN в зависимости от того, какая организация публикует документ [4].

4. ХАРАКТЕРИСТИКА ГРУПП СЕМИУРОВНЕВОЙ СИСТЕМЫ ДОКУМЕНТОВ МАНДАТА 460

Рассмотрим подробнее документы, представленные в каждой из областей

Группа 0 — рационализированная структура. Данная группа объединяет документы, описывающие способы рационализации структуры документов и стандартов в сфере ЭП.

На первом этапе был проведен анализ существующей структуры документов. Далее выполняются такие работы:

- обновление документов, которые касаются рационализированной структуры;
- исследования на предмет расширения перечня документов (рис. 4).

Группа 1 — создание и проверка ЭП. Данная группа включает документы и стандарты, описывающие правила и процедуры создания и проверки ЭП, форматы ЭП, а также профили защиты приложений при создании и проверки ЭП.

На первом этапе были проведены «быстрые исправления» в действующих документах для исключения дублирования. Второй этап включает в себя разработку новых документов:

- руководства для бизнес-сферы (TR 119 100);
- политика требований для создания/проверки ЭП (TS 119 101);

Rationalised structure for Electronic Signature Standardisation									
Sub-areas									
Guidance									
TR	1	19	0	0	0	Rationalised structure for Electronic Signature Standardisation			
TR	4	19	0	1	0	Rationalised structure for Electronic Signature Standardisation: Extended Rationalised structure including IAS			
SR	0	19	0	2	0	Rationalised structure for Electronic Signature Standardisation: Rationalised Framework of Standards for AdES in Mobile environments			
TR	4	19	0	3	0	Rationalised structure for Electronic Signature Standardisation: Best practices for SMEs			
TR	4	19	0	4	0	Rationalised structure for Electronic Signature Standardisation: Guidelines for citizens			
Policies									
TR	1	19	0	0	1	Rationalised Framework for Electronic Signature Standardisation: Definitions and abbreviations			

Рис. 4. Документы группы 0 [5]

- профили защиты для приложений создания/проверки ЭП (EN 419 111);
- форматы ЭП (внесены изменения в существующие стандарты типа EN);
- процедуры создания/проверки ЭП (EN 319 102);
- политика ЭП (изменён стандарт TS 119 172);
- тестирование и интероперабельность: форматы ЭП (TS 119 1x4) и форматы политик (TS 119 174) [5].

Группа 2 – устройства создания ЭП. На первом этапе разработки данной группы документов были проведены обновления требований к профилям защиты с учётом пересмотра стандарта (EN 419 211). Согласно требованиям стандарта сервер ЭП должен выглядеть, как показано на рис. 5.

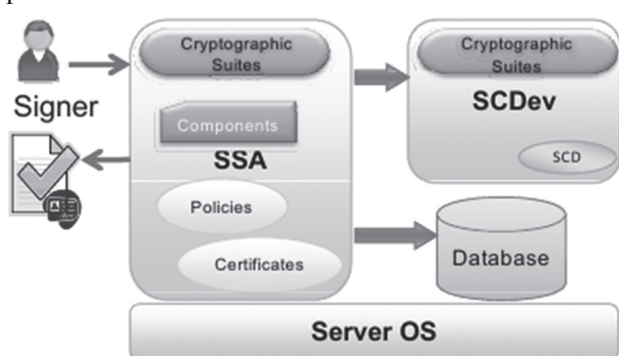


Рис. 5. Сервер подписи [5]

На последующих этапах работы были продолжены в таких направлениях:

- разработка стандарта метки времени (EN 419 231);
- разработка стандарта оценки и сертификации устройств создания подписей (EN 419 251);
- разработка стандарта SSSD интерфейса (EN 419 212).

В рамках этого направления работ также проходят исследования создания ЭП на мобильных устройствах и стандартизации требований для мобильных устройств.

Группа 3 – криптографические комплексы. В данную группу входят нормативные документы, которые описывают генерацию ключей, геш-функции, непосредственно алгоритмы ЭП и их форматы.

Первый этап нормализации завершился выходом обновленного стандарта TS 102 176-1.

На втором этапе был разработан и обновлен стандарт TS 119 312 – «Криптографические комплексы». В рамках данного стандарта был проведен анализ стойкости подписей на ближайшие 3–4 года, результаты которого приведены в табл. 1. Также разработаны руководства для использования ЭП в бизнес сфере (TR 119 300)[5].

Группа 4 – требования провайдеров доверительных электронных услуг. Основными работами по нормализации документов данной группы являются:

- разработка руководств (TR 119 400);
- оценка соответствия (Проект EN 319 403).

Также определены требования к провайдерам доверительных электронных услуг, которые используют ЭП. В результате пересмотрен стандарт «Общие требования» EN 319 401, пересмотрен стандарт «Квалифицированные сертификаты открытых ключей» EN 319 411, разработан проект стандарта «Сертификаты веб-сайтов» EN 319 411-1; разработан проект стандарта «Атрибуты сертификатов» EN 319 411-4; разработан проект стандарта «Метка времени» EN 319 421.

В дальнейшем планируется разработка нового объединенного стандарта «Сертификаты», который будет применяться для физических и юридических лиц, веб-сайтов, обеспечивая выпуск и обработку квалифицированных сертификатов.

Структура документов данной группы представлена на рис. 6.

Таким образом, можно выделить следующие тенденции стандартизации требований для провайдеров электронных доверительных услуг:

- 1) глобальное принятие стандартов для провайдеров электронных доверительных услуг в Европе, Северной Америке, Японии и т.д.;
- 2) необходимость оценки соответствия провайдеров по схемам, стандартизированным международными стандартами ISO 17065, 17021, 27006.
- 3) обеспечение регулярного пересмотра стандартов при наличии изменений в требованиях или важных условий.

Группа 5 – провайдеры приложений доверительных услуг. В этом направлении основные

Таблица 1

Анализ стойкости ЭП на ближайшие годы [5]

Entry name of the signature suite	1 years	3 years	6 years	10 years
sha256-with-rsa	1 536	2 048	2 048	not recommended
RSASSA-PSS with mgf1SHA-1Identifier	1 536	not recommended		
RSASSA-PSS with mgf1SHA-224Identifier	1 536	2 048	2 048	not recommended
RSASSA-PSS with mgf1SHA-256Identifier	1 536	2 048	2 048	3 072
sha224-with-ecdsa	224	224	not recommended	
sha256-with-ecdsa	256	256	256	256

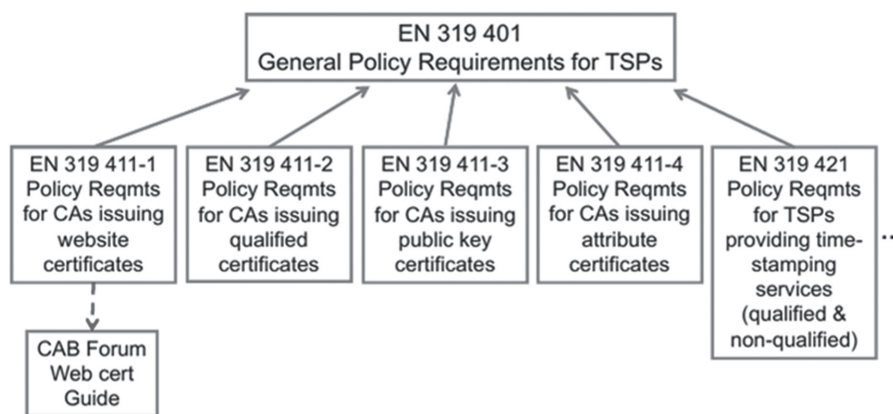


Рис. 6. Структура документов четвертой группы [5]

работы сводятся к разработке руководств для провайдеров (поставщиков) приложений доверительных услуг (TR 119 500) и исследованию необходимых аспектов внедрения стандартов электронной доставки (SR 019 530), а именно:

- обеспечение трансграничности услуги электронной доставки согласно Регламента-2014;
- внедрение стандартов идентификации отправителя;
- определение необходимого объема услуги электронной доставки.

На данный момент разработаны такие проекты стандартов:

- описание общей модели службы электронной доставки;
- анализ статуса стандартизации службы электронной доставки;
- предполагаемая структура стандартов.

Группа 6 – список статусов провайдеров электронных доверительных услуг. В соответствии с нормами Регламента 2014 в будущем должен быть сформирован список, который отражает статус провайдеров доверительных услуг, т.е. список доверия (trust list). Список является инструментом недопущения деятельности по предоставлению доверительных услуг провайдерами, которые не являются квалифицированными, а также инструментом предоставления актуальной информации обо всех доступных провайдерах электронных доверительных [2].

Основными направлениями стандартизации в этом направлении являются разработка «Руководства» (TR 119 600), разработка «Правил проверки соответствия провайдеров выдвинутым требованиям» (TS 119 614); разработка на формат списка доверия «Список доверия» (TS 119 612) [5].

ЗАКЛЮЧЕНИЕ

Таким образом, несмотря на многолетние исследования в ЕС и других технологически развитых государствах и союзах существует проблема нормализации нормативной базы в области электронных (цифровых) подписей. Ее разрешение даже на первом этапе позволит улучшить качество предоставляемых электронных доверительных услуг. Всем заинтересованным

сторонам, особенно разработчикам и пользователям будет легче ориентироваться в стандартах и нормативных документах. Также облегчиться контроль за исполнением требований действующего законодательства, появится возможность привлечения новых участников.

В целом, к сожалению, Мандат 460 только частично решает проблему законодательной путаницы. Тем не менее, на наш взгляд, необходимо для достижения конечного результата продолжать все начатые работы.

С точки зрения Украины участие в освоении, применении и совершенствовании этой нормативно-правовой базы позволит более оперативно двигаться к трансграничному электронному миру. Поэтому авторы надеются, что публикация этой статьи позволит рационально, и с лучшим качеством, решать возникшие проблемы.

Литература

- [1] Предложение Регламента Европейского парламента и Совета по вопросам идентификации и трастовых услуг для электронных операций на внутреннем рынке (2012).
- [2] Регламент Европейского парламента и Совета по вопросам идентификации и трастовых услуг для электронных операций на внутреннем рынке (2014).
- [3] Mandate M460: «Standardisation Mandate to The European Standardisation Organisations CEN, CENELEC and ETSI in the Field of Information and Communication Technologies Applied to Electronic Signatures».
- [4] Eesignature & Electronic Trust Services Standardisation Workshop-3rd December 2013 (Work Progress for Phase 2 of m460 Mandate).
- [5] Terms of Reference – Specialist Task Force 458 (TC ESI) Rationalised Framework for electronic signatures standards; Activities related to Signature Creation and Validation and Trusted Service Providers (TSP) supporting eSignatures.

Поступила в редколлегию 29.05.2014

Горбенко Юрий Иванович, фото и сведения об авторе см. на стр. 251.

Потий Александр Владимирович, фото и сведения об авторе см. на стр. 260.



Костенко Алексей Владимирович, заместитель начальника Управления функционирования центрального удостоверяющего органа Министерства юстиции Украины. Научные интересы: совершенствование законодательства и разработка совместных нормативно-правовых актов в сфере криптографической защиты информации и технической защиты информации.



Исирова Екатерина Владимировна, студентка 5 курса кафедры безопасности информационных систем и технологий ХНУ им. В. Н. Каразина. Научные интересы: защита информации в ИТС.

Горбенко Иван Дмитриевич, фото и сведения об авторе см. на стр. 216.

УДК 681.3.06(07)

Стан та сутність процесів нормалізації Європейської нормативної бази в області електронних підписів / Ю.І. Горбенко, О.В. Потій, О.В. Костенко, К.В. Ісірова, І.Д. Горбенко // Прикладна радіоелектроніка: наук.-техн. журнал. — 2014. — Том 13. — № 3. — С. 261–267.

Розглядаються процеси нормалізації Європейської нормативної бази в області електронних підписів. Аналізуються передумови проведення процесу нормалізації та результати робіт. Обговорюється нова схема нумерації документів, а також розглянуто кожну із предметних галузей використання.

Ключові слова: нормалізація Європейської нормативної бази в області електронних підписів, електронні довірчі (трастові) послуги, Мандат 460, структура нормативних документів в ЄС в області електронних підписів.

Табл.: 1. Іл.: 6. Бібліогр.: 5 найм.

UDC 681.3.06(07)

The state and main point of normalization processes of European regulatory framework in the sphere of electronic signatures / Yu.I. Gorbenko, A.V. Potiy, A.V. Kostenko, E.V. Isirova, I.D. Gorbenko // Applied Radio Electronics: Sci. Journ. — 2014. — Vol. 13. — № 3. — P. 261–267.

The normalization processes of European regulatory framework in the sphere of electronic signatures are considered. The causes of the normalization processes and the results of the work done are analyzed. A new numbering scheme of documents is discussed and each of the subject areas of application is described.

Keywords: normalization processes of European regulatory framework in the sphere of electronic signatures, electronic trust services, Mandate 460, structure of European regulatory documents in the sphere of electronic signatures.

Tab.: 1. Fig.: 6. Ref.: 5 items.