



**ЗАО «АВЕСТ»**

**Сравнение  
законодательств ЕС и РБ  
в области ЭЦП**

**Secur**  **IT** *conference* **у**

# История

## Европейский союз

Directive 1999/93/EC  
of the European Parliament  
and of the Council  
**of 13 December 1999**  
on a Community framework  
for electronic signatures

Regulation (EU) No 910/2014  
of the European Parliament  
and of the Council  
**of 23 July 2014**  
on electronic identification and  
trust services **(eIDAS)**  
for electronic transactions  
in the internal market and  
repealing Directive 1999/93/EC

## Республика Беларусь

Закон Республики Беларусь  
«Об электронном документе»  
от 10 января 2000 г. №357-3  
**принят 14 декабря 1999**

Закон Республики Беларусь  
«Об электронном документе и  
электронной цифровой подписи»  
**от 28.12.2009 г. № 113-3**

# Первое поколение законов

## Главный посыл: юридическая сила электронного документа

Электронный документ на машинном носителе приравнивается к документу на бумажном носителе и **имеет одинаковую с ним юридическую силу**

### **Directive 1999/93/EC on a Community framework for electronic signatures:**

- the electronic signature
- the advanced electronic signature
- the qualified certificate
  
- signature creation device

### **Закон Республики Беларусь «Об электронном документе»:**

- ↔ ЭЦП
- ↔ ЭЦП, карточка открытого ключа
- ↔ требования к деятельности по распространению открытых ключей
- ↔ средство ЭЦП

# Второе поколение законов: РБ

## Главный посыл: юридическая сила электронного документа

Электронный документ на машинном носителе приравнивается к документу на бумажном носителе и **имеет одинаковую с ним юридическую силу**

Directive 1999/93/EC  
on a Community framework  
for electronic signatures:

- the electronic signature
- the advanced electronic signature
- the qualified certificate
  
- signature creation device

Закон Республики Беларусь  
«Об электронном документе и  
ЭЦП»:

- ↔ ЭЦП
- ↔ ЭЦП, карточка открытого ключа
- ↔ **Сертификат открытого ключа  
ГосСУОК**
- ↔ средство ЭЦП

# Второе поколение законов: ЕС

## Главный посыл: идентификация и доверенные сервисы

### Электронная идентификация

- идентификация и аутентификация физических и юридических лиц
- различные уровни электронной идентификации
- наличие online сервиса идентификации

### Создание и проверка ЭЦП

#### Создание и проверка электронной печати

- ЭЦП юридического лица ↔ сертификат ЭЦП ГосСУОК + атрибутный сертификат ГосСУОК представителя юридического лица

### Создание и проверка меток времени

#### Квитирование доставки

#### Выпуск SSL сертификатов для аутентификации Web-сайтов

# Техническое регулирование: РБ

**ТР 2013/027/ВУ "Информационные технологии. Средства защиты информации. Информационная безопасность"**

**Положение о порядке КЗИ (приказ ОАЦ № 3 от 16.01.2015)**

- Рекомендованные криптографические алгоритмы и протоколы
- Требования безопасности к СКЗИ:
  - программным СКЗИ
  - программно-аппаратным СКЗИ
- Классификация СКЗИ и выделение требований к ним
  - Средство выработки ЭЦП
  - Средство проверки ЭЦП
- Требования к форматам электронных документов (ASN.1/CMS)

# Техническое регулирование: ЕС

ETSI Technical Committee Electronic Signatures: **Стандарты/профили ЕС**

## Стандартизация криптонаборов:

- Криптографические алгоритмы: 5 хэш-функций/6 алгоритмов ЭЦП
- Рекомендуемые длины ключей, сроки жизни ключей
- OID криптонаборов

## Стандартизация средств ЭЦП

- Профили защиты средств ЭЦП
- Профили защиты средств отметок времени
- Требования безопасности при управлении сертификатами
- ...

## Стандартизация форматов электронных документов

- Формат на основе ASN.1/CMS: CAdES
  - Профиль с отметкой времени для момента подписи
  - Профиль с включением информации об отзыве для офлайн проверки
  - Профили для ведения архива электронных документов
- Формат на основе XML: XAdES
- Формат на основе PDF: PAdES

# Техническое регулирование: ЕС

## **Требования к доверенным сервисам:**

- Политики и регламенты сервисов
- Профили сервисов
- ...

## **Требования к поставщикам доверенных сервисов:**

- Требования к поставщикам услуг электронной почты
- Требования к поставщикам услуг хранения данных

## **Список доверенных поставщиков доверенных сервисов**

- Выпускается национальным регулятором
- Формат на основе ASN.1/CMS





**Спасибо за внимание!**

**[www.avest.by](http://www.avest.by)**

**[welcome@avest.by](mailto:welcome@avest.by)**

**+375 17 207-92-34**